PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-073424
(43)Date of publication of application : 12.03.2002

(51)Int.Cl G06F 12/14
G06K 17/00
G06K 19/00
H04Q 7/38
H04L 9/32

(21)Application number : 2000-262445
(22)Date of filing : 31.08.2000

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : MAEDA SHIGENOBU

(54) SEMICONDUCTOR DEVICETERMINAL DEVICE AND COMMUNICATION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a semiconductor devicea terminal device and a correspondence procedure capable of heighten technical barrier to abuse of application instruments by changing semiconductor board.
SOLUTION: A code generating part 400 generates a specific identifying code Cd in a semiconductor board CH1 (or CH3). A memory 601 that is formed in another semiconductor board CH2 stores identifying code Cd as memory code Co. When semiconductor device 600 is shipped as productidentifying code Cd is written into the memory 601 from the code generating part 400. A comparing circuit 403 compares identifying code Cd with memory code Co and makes one of the operation in a specified circuit stopif both identifying code Cd and memory code Co don't agree each other.

CLAIMS

[Claim(s)]
[Claim 1]A code generating part which is formed in each of at least one semiconductor substrateand generates an identification signal peculiar to the semiconductor substratesaid identification signal -- respectively -- a semiconductor device provided with a memory which memorizes numerals which are in agreement

with an identification signal which is alikeis formed in a semiconductor substrate other than a corresponding semiconductor substrateand corresponds as a memory code.
[Claim 2]The semiconductor device according to claim 1 with which said memory is provided with OTPROM which memorizes said memory code.
[Claim 3]So that said code generating part may originate in dispersion in the electrical property of a semiconductor device and said semiconductor device and a value may varyThe semiconductor device according to claim 1 or 2 which generates said identification signal and is provided with a coding circuit to output by changing the electrical property of said semiconductor device into a signal of digital format.
[Claim 4]The semiconductor device according to claim 3 with which said semiconductor device has the polycrystalline substanceand dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[Claim 5]The semiconductor device according to claim 1 or 2 with which said code generating part is provided with OTPROM which memorizes said identification signal.
[Claim 6]said identification signal -- respectively -- the semiconductor device according to any one of claims 1 to 5 which is alikecompares said identification signal with said corresponding memory codejudges whether these both sides are in agreementand is further provided with a comparison circuit which outputs a decision signal expressing the result.
[Claim 7]The semiconductor device according to claim 6 currently formed in said semiconductor substrate corresponding to an identification signal which said comparison circuit makes a comparison object.
[Claim 8]said identification signal -- respectively -- it has further a key generation partan enciphering circuitand a decoding circuit which were alike and were formed in said corresponding semiconductor substrateand said key generation partGenerate a key for encryption peculiar to said corresponding semiconductor substrateand said enciphering circuitSaid identification signal which said code generating part formed in said corresponding semiconductor substrate generatesTell to said memory which enciphers based on said corresponding key and corresponds in enciphered formand said corresponding memoryMemorize said identification signal in enciphered form which said enciphering circuit outputs as said memory code in enciphered formand said decoding circuitBased on said corresponding keydecrypt said enciphered memory code which is memorized by said corresponding memoryand said comparison circuitThe semiconductor device according to claim 7 which compares said identification signal which said corresponding coding circuit generates with said decrypted memory code which said corresponding decoding circuit generates.
[Claim 9]The semiconductor device comprising according to claim 8:
Semiconductor device with said another key generation part.
Another coding circuit which generates and outputs said key by changing the electrical property of said semiconductor device into a signal of digital format so that

it may originate in dispersion in the electrical property of said another semiconductor device and a value may vary.

[Claim 10]The semiconductor device according to claim 9 with which said another semiconductor device has the polycrystalline substanceand dispersion in said electrical property of said another semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[Claim 11]The semiconductor device according to claim 8 with which said key generation part is provided with OTPROM which memorizes said key.
[Claim 12]said identification signal -- respectively -- it being alikebeing formed in said corresponding semiconductor substrateand with sending out in said memory to which said identification signal which said corresponding coding circuit generated corresponds. The semiconductor device according to any one of claims 7 to 11 further provided with a switching circuit which performs exclusively an input to said comparison circuit of said memory code memorized by said corresponding memory.
[Claim 13]The semiconductor device according to any one of claims 6 to 12 further provided with a prescribed circuit containing a circuit part which is operation or un-operating selectively depending on said decision signal corresponding to each of said identification signal.
[Claim 14]The semiconductor device according to claim 13 with which said prescribed circuit is formed in one of said the at least one semiconductor substrate in which said comparison circuit is formed.
[Claim 15]The semiconductor device according to any one of claims 1 to 14 with the single number of said at least one semiconductor substrate.
[Claim 16]the number of said at least one semiconductor substrate is two pieces -- said identification signal -- respectively -- the semiconductor device according to any one of claims 1 to 14 with which it is alike and said corresponding code generating part and said memory of each other are formed in one side and another side of said two semiconductor substrates.
[Claim 17]A terminal unit comprising:
A key generation part which generates a key for encryption and is provided with a coding circuit to output by changing the electrical property of said semiconductor device into a signal of digital format so that it may originate in dispersion in the electrical property of a semiconductor device and the semiconductor device concerned and a value may vary.
An enciphering circuit which enciphers send data based on said keyand a decoding circuit which decrypts received data based on said key.

[Claim 18]The terminal unit according to claim 17 which said coding circuit and said decoding circuit are included in a body partand is built into an auxiliary section which said key generation part can desorb freely to said body part.

[Claim 19]The terminal unit according to claim 18 in which said auxiliary section is an IC card.
[Claim 20]The terminal unit according to any one of claims 17 to 19 with which said semiconductor device has the polycrystalline substanceand dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[Claim 21]Have the semiconductor device according to claim 13 or 14and said prescribed circuitA terminal unit which is a communication circuit which transmits and receives a signal between the exteriorsand stops either [at least] transmission or reception when disagreement between at least one each of said identification signal of said decision signal and said corresponding memory code is shown.
[Claim 22]A terminal unit which is provided with the semiconductor device according to any one of claims 6 to 12 and a communication circuit which transmits and receives a signal between the exteriors and with which said communication circuit transmits each of said decision signal to said exterior as said a part of signal.
[Claim 23]A terminal unit which is provided with the semiconductor device according to any one of claims 1 to 5 and a communication circuit which transmits and receives a signal between the exteriors and with which said communication circuit transmits each of said identification signaland each of said memory code to said exterior as said a part of signal.
[Claim 24]The terminal unit according to claim 23 which the number of said at least one semiconductor substrate is singleand each and said communication circuit of said code generating part are included in a body partand is built into an auxiliary section which each of said memory can desorb freely to said body part.
[Claim 25]The 1st key generation part that generates the 1st key for encryption in said body partthe 1st enciphering circuit that enciphers said identification signal which said code generating part generates based on said 1st keyand ** -- it being incorporated and to said auxiliary section. The 2nd key generation part that generates the 2nd key for encryptionand the 2nd enciphering circuit that enciphers said memory code which said memory memorizes based on said 2nd key** -- it being incorporated and said 1st enciphering circuitThe terminal unit according to claim 24 which also enciphers said memory code which said 2nd enciphering circuit enciphered based on said 1st keyand said communication circuit is the form enciphered in said 1st enciphering circuitand transmits said identification signal and said memory code to said exterior.
[Claim 26]The terminal unit according to claim 25 with which said 1st key generation part and said 1st enciphering circuit are formed in said semiconductor substrate in which said coding circuit was formed.
[Claim 27]The terminal unit according to claim 25 or 26 with which said 2nd key generation part and said 2nd enciphering circuit are formed in said semiconductor substrate in which said memory was formed.

[Claim 28]The terminal unit according to any one of claims 24 to 27 which is a battery charger which charges said cell by providing said body part with a cell which can be chargedand equipping said body part with said auxiliary section.
[Claim 29]The terminal unit according to any one of claims 24 to 27 with which said auxiliary section is an IC cardand a communication interface for carrying transmission of numerals from said auxiliary section to said body part on radio is further built into each of said body part and said auxiliary section.
[Claim 30]The terminal unit according to any one of claims 22 to 29 with which said communication circuit is formed in one of said the at least one semiconductor substrate with said code generating part.
[Claim 31]A terminal unit provided with a communication circuit which performs radio which carried communication enterprise equipmentand a wireless communication network circuit which performs radio by forming a wireless communication network which does not carry said communication enterprise equipment.
[Claim 32]By performing connection and cutting of a course of signal transmission between said communication circuit and said wireless communication network circuitenabling free selectionThe terminal unit according to claim 31 further provided with a switching circuit which realizes relay of communication of two or more others other than communication between a user of said terminal unit which leads said wireless communication networkand the othersand a user of said terminal unit which leads said wireless communication network enabling free selection.
[Claim 33]A key generation part which generates a key for encryptionand an enciphering circuit which enciphers a sending signal sent to said wireless communication network circuit based on said key from said communication circuit in said signal transmissionA decoding circuit which decrypts an input signal sent to said communication circuit based on said key from said wireless communication network circuit in said signal transmissionA code generating part which generates numerals to prepare for a pan and for said key generation part identify said terminal unitThe terminal unit according to claim 32 provided with key operation part which computes a common key usable in common between said user and said communications partner based on said numerals which said code generating part generatesand another numerals sent from a communications partner through said wireless communication network circuit.
[Claim 34]The terminal unit according to claim 33 which generates said numerals and is provided with a coding circuit to output by changing the electrical property of said semiconductor device into a signal of digital format so that said code generating part may originate in dispersion in the electrical property of a semiconductor device and said semiconductor device and a value may vary.
[Claim 35]The terminal unit according to claim 34 with which said semiconductor device has the polycrystalline substanceand dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said

polycrystalline substance.
[Claim 36]The terminal unit according to claim 33 with which said code generating part is provided with OTPROM which memorizes said numerals.
[Claim 37]In said signal transmissionfrom said wireless communication network circuithave further the 1st and 2nd mixers inserted in a course of an input signal sent to said communication circuitand said 1st mixerThe terminal unit according to any one of claims 32 to 36 which restores to an input signal which said communication circuit receivedand modulates said input signal which restored to said 2nd mixer using a subcarrier which has the frequency in a frequency band of said communication circuit.
[Claim 38]A correspondence procedure with which entrepreneur equipment characterized by comprising the following and the terminal unit according to claim 22 communicate mutually.
(a) A process at which said terminal unit transmits each of said decision signal to said entrepreneur equipment.
(b) An attestation process which does not perform said attestation if conditions that each of said decision signal which said entrepreneur equipment received shows coincidence with each of said identification signal and said corresponding memory code are satisfieda user of said terminal unit will perform attestation that he is a just user and said conditions will not be satisfied.

[Claim 39]A correspondence procedure with which entrepreneur equipment characterized by comprising the following and the terminal unit according to claim 23 communicate mutually.
(a) A process at which said terminal unit transmits each of said identification signaland each of said memory code to said entrepreneur equipment.
(b) A process of judging whether it being in agreement as compared with said memory code with which said entrepreneur equipment corresponds each of said identification signal which received(c) An attestation process which does not perform said attestation if conditions of having judged with said entrepreneur equipment being in agreement with said memory code with which each of said identification signal corresponds in said process (b) are satisfieda user of said terminal unit will perform attestation that he is a just user and said conditions will not be satisfied.

[Claim 40](e) The correspondence procedure according to claim 39 further provided with a process on which said entrepreneur equipment records each of said identification signal which receivedand each of said memory code.
[Claim 41]The correspondence procedure according to claim 39 which records each of said identification signal which receivedand each of said memory code in said process (c) when said entrepreneur equipment does not perform said attestation.
[Claim 42]A correspondence procedure comprising:

(a) A process which entrepreneur equipment acquires said identification signal of the terminal unit according to claim 24and memorizes as the 1st registration code (b) A process which said entrepreneur equipment obtains said memory code of said terminal unitand memorizes as the 2nd registration code(c) After said process (a) and (b)said entrepreneur equipment and said terminal unit are provided with a communicating process which communicates mutuallyand it the communicating process (c) concerned(c-1) The 1st communicating process performed when said body part is not equipped with said auxiliary section(c-2) Have the 2nd communicating process performed when said body part is equipped with said auxiliary sectionand said 1st communicating process (c-1)(c-1-1) A process at which said terminal unit transmits said identification signal to said entrepreneur equipment(c-1-2) A process of judging whether said entrepreneur equipment comparing said received identification signal with said 1st registration codeand these both sides being in agreement(c-1-3) If conditions that said entrepreneur equipment judged with said both sides being in agreement at said process (c-1-2) are satisfiedA process at which it has an attestation process which does not perform said attestationandas for said 2nd communicating process (c-2)said (c-2-1) terminal unit transmits said identification signal and said memory code to said entrepreneur equipment if a user of said terminal unit performs attestation that he is a just user and said conditions are not satisfied(c-2-2) While judging whether said entrepreneur equipment compares said received identification signal with said 1st registration codeand these both sides are in agreementA process of judging whether said received memory code being compared with said 2nd registration codeand these both sides being in agreement(c-2-3) If conditions that a judgment that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-2-2) was obtained are satisfiedA high rank attestation process of not performing said high-ranking attestation if a user of said terminal unit performs high-ranking attestation that he is a just user and said conditions are not satisfied.

[Claim 43]The correspondence procedure according to claim 42 from which entrepreneur equipment obtains said memory code of said terminal unit when said entrepreneur equipment and said terminal unit communicatewhere said body part is equipped [said process (b)] with said auxiliary section.
[Claim 44]Said process (c) is performed when said body part is equipped with said (c-3) auxiliary sectionand it is further provided with a change process of changing said 2nd registration codeand it said change process (c-3)(c-3-1) Said terminal unit with a requirement signal expressing volition of said change. While judging whether a process of transmitting said identification signal and said memory code to said entrepreneur equipmentand said identification signal which said (c-3-2) entrepreneur equipment received are compared with said 1st registration codeand these both sides are in agreementA process of judging whether said received memory code being compared

with said 2nd registration codeand these both sides being in agreement(c-3-3) A process to which said change is permitted whenever it obtained a decision result that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-3-2)(c-3-4) A process of exchanging said auxiliary section of said terminal unitand equipping with an auxiliary section after exchange after said process (c-3-3) to said body part(c-3-5) A process at which said terminal unit transmits said identification signal and said memory code after change based on said auxiliary section after exchange to said entrepreneur equipment after said process (c-3-4)and said (c-3-6) entrepreneur equipmentThe correspondence procedure according to claim 42 or 43 provided with a process of updating said 2nd registration code with said memory code after change received only within a case where said change is permittedat said process (c-3-3).

[Claim 45]A correspondence procedure comprising:

(a) A process which entrepreneur equipment obtains said identification signal and said 1st key of the terminal unit according to claim 25and memorizes as the 1st registration code and a registration keyrespectively

(b) A process which said entrepreneur equipment obtains said memory code enciphered with said 2nd key of said terminal unitand memorizes as the 2nd registration code(c) After said process (a) and (b)said entrepreneur equipment and said terminal unit are provided with a communicating process which communicates mutuallyand it the communicating process (c) concerned(c-1) The 1st communicating process performed when said body part is not equipped with said auxiliary section(c-2) Have the 2nd communicating process performed when said body part is equipped with said auxiliary sectionand said 1st communicating process (c-1)(c-1-1) Said terminal unit in form enciphered in said 1st enciphering circuit. A process of transmitting said identification signal to said entrepreneur equipmentand after said (c-1-2) entrepreneur equipment decrypts said received identification signal based on said registration keyIf a process of judging whether these both sides being in agreementand conditions that said (c-1-3) entrepreneur equipment judged with said both sides being in agreement at said process (c-1-2) are satisfied as compared with said 1st registration codeIf a user of said terminal unit performs attestation that he is a just user and said conditions are not satisfiedhave an attestation process which does not perform said attestation and said 2nd communicating process (c-2)(c-2-1) Said terminal unit in form enciphered in said 1st enciphering circuit. A process of transmitting said identification signal and a memory code to said entrepreneur equipmentand after said (c-2-2) entrepreneur equipment decrypts said received identification signal based on said registration keyWhile judging whether these both sides are in agreement as compared with said 1st registration codeA process of judging whether these both sides being in agreement as compared with said 2nd registration code after decrypting said received memory code based on said registration key(c-2-3) If conditions that a judgment that said entrepreneur

equipment is in agreement also in any of two judgments of said process (c-2-2) was obtained are satisfiedA high rank attestation process of not performing said high-ranking attestation if a user of said terminal unit performs high-ranking attestation that he is a just user and said conditions are not satisfied.

[Claim 46]The correspondence procedure according to claim 45 from which entrepreneur equipment obtains said memory code enciphered with said 2nd key of said terminal unit when said entrepreneur equipment and said terminal unit communicatewhere said body part is equipped [said process (b)] with said auxiliary section.
[Claim 47]The correspondence procedure comprising according to claim 45 or 46: Said process (c) is performed when said body part is equipped with said (c-3) auxiliary sectionand it is further provided with a change process of changing said 2nd registration codeand it said change process (c-3)(c-3-1) A process from which said terminal unit transmits said identification signal and said memory code to said entrepreneur equipment in form enciphered with a requirement signal expressing volition of said change in said 1st enciphering circuit.
(c-3-2) After said entrepreneur equipment decrypts said received identification signal based on said registration keyA process of judging whether these both sides being in agreement as compared with said 2nd registration code after decrypting said received memory code based on said registration keywhile judging whether these both sides having been in agreement as compared with said 1st registration code.
(c-3-3) A process to which said change is permitted whenever it obtained a decision result that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-3-2).
(c-3-4) A process of exchanging said auxiliary section of said terminal unitand equipping with an auxiliary section after exchange after said process (c-3-3) to said body part(c-3-5) Said terminal unit in form enciphered in said 1st enciphering circuit after said process (c-3-4). A process of transmitting said identification signal and said memory code after change based on said auxiliary section after exchange to said entrepreneur equipment(c-3-6) A process of updating said 2nd registration code with numerals obtained when said entrepreneur equipment decrypts said memory code after change received only within a case where said change is permittedat said process (c-3-3) based on said registration key.

[Claim 48]The correspondence procedure according to any one of claims 42 to 47 which records each numerals made into an object of comparison with each registration code at said process (c-2-2) in said high rank attestation process when said entrepreneur equipment does not perform said high-ranking attestation.
[Claim 49]The correspondence procedure according to any one of claims 42 to 48 which records telex rate gold to communication before it in said high rank attestation

process as what was able to be supported when said entrepreneur equipment performs said high-ranking attestation.
[Claim 50]In said high rank attestation processsaid entrepreneur equipmentThe correspondence procedure according to any one of claims 42 to 49 which it records having performed the high-ranking attestation concerned when performing said high-ranking attestationand said entrepreneur equipment makes it further conditions to record having performed said high-ranking attestation in said attestation processand performs said attestation.
[Claim 51]In said high rank attestation processsaid entrepreneur equipmentIn recording as that in which a commercial transaction performed by communication before it was materialized when said high-ranking attestation was performed and not performing said high-ranking attestationThe correspondence procedure according to any one of claims 42 to 50 recorded as that in which said commercial transaction performed by communication before it was not materialized.
[Claim 52]The correspondence procedure according to any one of claims 38 to 51 which said entrepreneur equipment continues said communication in said attestation process when performing said attestationand stops said communication in not performing said attestation.
[Claim 53]In space through which a crowd who carries a terminal unit in which radio which carried communication enterprise equipment and formation of a wireless communication network which does not carry said communication enterprise equipment are possible gathers thru/or passesA correspondence procedure which enabled communication of said terminal units in said Sorama's inside even if a field which cannot perform said radio which carried said communication enterprise equipment by forming said wireless communication network between said terminal units which two or more [in said crowd / at least some] carry was in said Sorama.
[Claim 54]Said some of two or more terminal units which form said wireless communication network by performing said radio which carried said communication enterprise equipmentThe correspondence procedure according to claim 53 to which said some of two or more of other terminal units which form said wireless communication network made it possible to also perform communication which carried said wireless communication network and carried said communication enterprise equipment further.
[Claim 55]They are said at least some of two or more terminal units which form said wireless communication networkThe correspondence procedure according to claim 53 or 54 which a terminal unit of a lot which carries said wireless communication network and communicates mutually computes a common key by exchanging mutually numerals which identify eachand exchanges signal transmission in form enciphered based on the common key concerned.
[Claim 56]The correspondence procedure according to any one of claims 53 to 55 which enabled communication which carried said wireless communication network only

within urgent emergency traffic.
[Claim 57]Install said radio which carried said communication enterprise equipment for another terminal unit which can form said wireless communication network in said field which cannot be performedand by that causeThe correspondence procedure according to any one of claims 53 to 56 which enabled formation of said wireless communication network even when density of said crowd who carries said terminal unit was low.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to a semiconductor devicea terminal unitand a correspondence procedure.
[0002]
[Description of the Prior Art]It is made to look as if it was others' terminal unit in the communication network about the self terminal unit by changing the unauthorized use of terminal unitssuch as a portable telephonei.e.an identification numberetc.and crimessuch as escaping the obligation to pay a feeare said to increase in recent years. Though this unauthorized use is naturalshould be socially regulated through legal punishment like other crimesbut. When making it difficult to use improperly technically simultaneouslyi.e.raise the technical barrier (security) to an unauthorized useprevents a crimethey are especially recognized to be one of the important measures.
[0003]Drawing 64 is an explanatory view quoted from the "Nikkei electronics" February 81999 item (no.736) and the report published by pp.155-162 (followingdocument 1).
An example of the measure against dishonesty prevention implemented about the portable telephone now is shown.
The methods of drawing 64 are the method that security is the highestand **********in the present measure against dishonesty prevention so that it may be indicated in document 1.
The procedure of attestation" is used.

[0004]In this methodthe serial number of a portable telephone (ESN:Electronic Serial Number)The shared secrecy data (SSD:Shared Secret Data) which a portable telephone and the authentication center of a communication enterprise shareand a mobile identification number (MIN:Mobile Identification Number) are given for every portable telephone. These identification numbers are coded to the code called AUTHREQ based on a CAVE (Cellular Authentication andVoice Encryption) algorithm. The random number called RAND outputted from the mobile switching center of a

communication enterprise in the case of encryption is used.
[0005]A communication enterprise decrypts the code AUTHREQ transmitted from the portable telephone based on a CAVE algorithm. The identification number produced by being decrypted is compared with the identification number containing the shared secrecy data SSD which only an authentication center graspsand the judgment of communicative permission or disapproval is made according to the result. Thusbased on the shared secrecy data SSD shared only between a portable telephone and a communication enterprisethe check of whether the user of a portable telephone is a just useri.e.attestationis performed.
[0006]
[Problem(s) to be Solved by the Invention]Howeverthe crime of using improperly by exchanging this attestation also to the authentic method of drawing 64 it is supposed that it is the most powerful measure against dishonesty prevention in present is said to spread. the identification number given to a portable telephone is said to be in being written in the rewritable flash memory (flash ROM) so that one of technical causes may be indicated also in document 1.
[0007]Drawing 65 is a block diagram showing the internal configuration of a portable telephone briefly. The conventional portable telephone 903 is equipped with the flash memory 908 with the communication circuit 907. The communication circuit 907 operates according to the program written in the flash memory 908. The identification number is also held at the flash memory 908and the communication circuit 907 codes based on identification number ID read from the flash memory 908and transmits the code AUTHREQ generated by coding to a communication enterprise.
[0008]As a storagethe rewritable flash memory 908 is used because it needs to correspond to program change which a communication enterprise makesfor examplethe change to the program compatible with a new communication methodetc. In the process in which it not only cannot respond to program changebut it will manufacture a mask ROM if the mask ROM which is not rewritable is used. It is because it is necessary to record an identification number and the decline in manufacturing efficiency and the rise of a manufacturing cost are brought about using a different mask pattern corresponding to a different identification number for every individual.
[0009]The application (Tokuganhei11-178173; followingdocument 2) previously made by applicant of this applicationThe art of removing the above-mentioned cause is indicated by forming in a semiconductor substrate the semiconductor device which has the polycrystalline substanceand using dispersion in the electrical property originating in dispersion in the crystal structure of the polycrystalline substance for generation of an identification number.
[0010]Not only the gestalt performed by rewriting an identification number as an unauthorized use of a terminal unit on the other hand but the gestalt performed by exchanging unjustly the semiconductor substrate (semiconductor chip) carried in the

terminal unit is known. That isby exchanging the semiconductor substrate on which a certain identification number was recorded to the semiconductor substrate on which another identification number was recordedit made a show like and the gestalt of an unauthorized use of escaping the obligation to pay a fee has also appeared [which is others' terminal unit] the self terminal unit. Not only a terminal unit but the crime of acquiring an illegal profit by using improperly by exchanging a semiconductor substrate in the applied machine of a common semiconductor device including the game machine (the game machine by which a common name is carried out to a "pachinko stand" in our country is the example of representation) etc. which have gamble naturefor example is known.

[0011]In the portable terminal unit (namelyportable telephone) which carries communication enterprise equipment and performs radiothe gestalt of the unauthorized use of escaping the obligation to pay a fee is also known [the loss]using the terminal unit.

[0012]This invention is what was made in order to cancel the above-mentioned problem in a Prior artIt aims at acquiring the semiconductor deviceterminal unitand correspondence procedure which can raise the technical barrier to an unauthorized use with various gestaltenand aims at providing the terminal unit and correspondence procedure which improved the convenience in radio by using such art further.

[0013]

[Means for Solving the Problem]A code generating part which a device of the 1st invention is formed in each of at least one semiconductor substrate in a semiconductor deviceand generates an identification signal peculiar to the semiconductor substratesaid identification signal -- respectively -- it is alikeis formed in a semiconductor substrate other than a corresponding semiconductor substrateand has a memory which memorizes numerals which are in agreement with a corresponding identification signal as a memory code.

[0014]In a device of the 2nd inventionsaid memory is provided with OTPROM which memorizes said memory code in a semiconductor device of the 1st invention.

[0015]In a semiconductor device of the 1st or the 2nd invention with a device of the 3rd inventionBy changing the electrical property of said semiconductor device into a signal of digital formatsaid identification signal is generated and it has a coding circuit to output so that said code generating part may originate in dispersion in the electrical property of a semiconductor device and said semiconductor device and a value may vary.

[0016]In a device of the 4th inventionin a semiconductor device of the 3rd inventionsaid semiconductor device has the polycrystalline substance and dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.

[0017]In a device of the 5th inventionsaid code generating part is provided with OTPROM which memorizes said identification signal in a semiconductor device of the

1st or the 2nd invention.
[0018]setting a device of the 6th invention to a semiconductor device of the 1st thru/or the 5th one of inventions -- said identification signal -- respectively -- it is alikesaid identification signal is compared with said corresponding memory codeand it judges whether these both sides are in agreementand has further a comparison circuit which outputs a decision signal expressing the result.
[0019]In a device of the 7th inventionsaid comparison circuit is formed in said semiconductor substrate corresponding to an identification signal made into a comparison object in a semiconductor device of the 6th invention.
[0020]setting a device of the 8th invention to a semiconductor device of the 7th invention -- said identification signal -- respectively -- it being alike andHave further a key generation partan enciphering circuitand a decoding circuit which were formed in said corresponding semiconductor substrateand said key generation partGenerate a key for encryption peculiar to said corresponding semiconductor substrateand said enciphering circuitSaid identification signal which said code generating part formed in said corresponding semiconductor substrate generatesTell to said memory which enciphers based on said corresponding key and corresponds in enciphered formand said corresponding memoryMemorize said identification signal in enciphered form which said enciphering circuit outputs as said memory code in enciphered formand said decoding circuitDecrypting said enciphered memory code which is memorized by said corresponding memory based on said corresponding keysaid comparison circuit compares said identification signal which said corresponding coding circuit generates with said decrypted memory code which said corresponding decoding circuit generates.
[0021]So that said key generation part may originate in dispersion in the electrical property of another semiconductor device and said another semiconductor device and a value may differ in a device of the 9th invention in a semiconductor device of the 8th inventionBy changing the electrical property of said semiconductor device into a signal of digital formatsaid key is generated and it has another coding circuit to output.
[0022]In a device of the 10th inventionin a semiconductor device of the 9th inventionsaid another semiconductor device has the polycrystalline substanceand dispersion in said electrical property of said another semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[0023]In a device of the 11th inventionsaid key generation part is provided with OTPROM which memorizes said key in a semiconductor device of the 8th invention.
[0024]In a semiconductor device of the 7th thru/or the 11th one of inventions a device of the 12th inventionsaid identification signal -- respectively -- it being alikebeing formed in said corresponding semiconductor substrateand with sending out in said memory to which said identification signal which said corresponding coding circuit generated corresponds. It has further a switching circuit which performs exclusively an input to said comparison circuit of said memory code memorized by

said corresponding memory.
[0025]A device of the 13th invention is further provided with a prescribed circuit containing a circuit part which is operation or un-operating selectively depending on said decision signal corresponding to each of said identification signal in a semiconductor device of the 6th thru/or the 12th one of inventions.
[0026]In a device of the 14th inventionsaid prescribed circuit is formed in one of said the at least one semiconductor substrate in which said comparison circuit is formed in a semiconductor device of the 13th invention.
[0027]In a semiconductor device of the 1st thru/or the 14th one of inventions in a device of the 15th inventionthe number of said at least one semiconductor substrate is single.
[0028]In a semiconductor device of an invention boiled in the 1st thru/or the 14th any in a device of the 16th inventionthe number of said at least one semiconductor substrate is two pieces -- said identification signal -- respectively -- it is alike and said corresponding code generating part and said memory of each other are formed in one side and another side of said two semiconductor substrates.
[0029]A device of the 17th invention is a terminal unit and a key for encryption is generated by changing the electrical property of said semiconductor device into a signal of digital format so that it may originate in dispersion in the electrical property of a semiconductor device and the semiconductor device concerned and a value may varyIt has a key generation part provided with a coding circuit to outputan enciphering circuit which enciphers send data based on said keyand a decoding circuit which decrypts received data based on said key.
[0030]In a device of the 18th inventionin a terminal unit of the 17th inventionsaid coding circuit and said decoding circuit are included in a body partand said key generation part is included in an auxiliary section which can be freely desorbed to said body part.
[0031]In a device of the 19th inventionsaid auxiliary section is an IC card in a terminal unit of the 18th invention.
[0032]In a device of the 20th inventionin a terminal unit of the 17th thru/or the 19th one of inventionssaid semiconductor device has the polycrystalline substance and dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[0033]A device of the 21st invention is a terminal unit and is provided with a semiconductor device of the 13th or the 14th inventionSaid prescribed circuit is a communication circuit which transmits and receives a signal between the exteriorsand when disagreement between at least one each of said identification signal of said decision signal and said corresponding memory code is showneither [at least] transmission or reception is stopped.
[0034]A device of the 22nd invention is a terminal unitit has a semiconductor device of the 6th thru/or the 12th one of inventionsand a communication circuit which

transmits and receives a signal between the exteriorsand said communication circuit transmits each of said decision signal to said exterior as said a part of signal.
[0035]A device of the 23rd invention is a terminal unitit has a semiconductor device of the 1st thru/or the 5th one of inventionsand a communication circuit which transmits and receives a signal between the exteriorsand said communication circuit transmits each of said identification signaland each of said memory code to said exterior as said a part of signal.
[0036]In a device of the 24th inventionin a terminal unit of the 23rd inventionthe number of said at least one semiconductor substrate is singleeach and said communication circuit of said code generating part are included in a body partand each of said memory is included in an auxiliary section which can be freely desorbed to said body part.
[0037]In a device of the 25th inventionin a terminal unit of the 24th inventionto said body part. The 1st key generation part that generates the 1st key for encryptionand the 1st enciphering circuit that enciphers said identification signal which said code generating part generates based on said 1st key** -- it being incorporated and to said auxiliary section. The 2nd key generation part that generates the 2nd key for encryptionand the 2nd enciphering circuit that enciphers said memory code which said memory memorizes based on said 2nd keyIt is incorporated and ** and also said memory code which said 2nd enciphering circuit enciphered in said 1st enciphering circuit are also enciphered based on said 1st keyand said communication circuit is the form enciphered in said 1st enciphering circuitand transmits said identification signal and said memory code to said exterior.
[0038]In a device of the 26th inventionsaid 1st key generation part and said 1st encipher ng circuit are formed in said semiconductor substrate in which said coding circuit was formed in a terminal unit of the 25th invention.
[0039]In a device of the 27th inventionsaid 2nd key generation part and said 2nd enciphering circuit are formed in said semiconductor substrate in which said memory was formed in a terminal unit of the 25th or the 26th invention.
[0040]In a device of the 28th inventionin a terminal unit of the 24th thru/or the 27th one of inventionssaid body part is provided with a cell which can be chargedand said auxiliary section is a battery charger which charges said cell by equipping said body part.
[0041]In a device of the 29th inventionin a terminal unit of the 24th thru/or the 27th one of inventionssaid auxiliary section is an IC card and a communication interface for carrying transmission of numerals from said auxiliary section to said body part on radio is further built into each of said body part and said auxiliary section.
[0042]In a device of the 30th inventionsaid communication circuit is formed in one of said the at least one semiconductor substrate with said code generating part in a terminal unit of the 22nd thru/or the 29th one of inventions.
[0043]A device of the 31st invention is a terminal unit and is provided with a

communication circuit which performs radio which carried communication enterprise equipmentand a wireless communication network circuit which performs radio by forming a wireless communication network which does not carry said communication enterprise equipment.
[0044]In a terminal unit of the 31st inventiona device of the 32nd invention by performing connection and cutting of a course of signal transmission between said communication circuit and said wireless communication network circuitenabling free selectionIt has further a switching circuit which realizes relay of communication of two or more others other than communication between a user of said terminal unit which leads said wireless communication networkand the othersand a user of said terminal unit which leads said wireless communication network enabling free selection.
[0045]A key generation part in which a device of the 33rd invention generates a key for encryption in a terminal unit of the 32nd inventionAn enciphering circuit which enciphers a sending signal sent to said wireless communication network circuit based on said key from said communication circuit in said signal transmissionA decoding circuit which decrypts an input signal sent to said communication circuit based on said key from said wireless communication network circuit in said signal transmissionA code generating part which generates numerals to prepare for a pan and for said key generation part identify said terminal unitBased on said numerals which said code generating part generatesand another numerals sent from a communications partner through said wireless communication network circuitit has key operation part which computes a common key usable in common between said user and said communications partner.
[0046]So that said code generating part may originate in dispersion in the electrical property of a semiconductor device and said semiconductor device and a value may differ in a device of the 34th invention in a terminal unit of the 33rd inventionBy changing the electrical property of said semiconductor device into a signal of digital formatsaid numerals are generated and it has a coding circuit to output.
[0047]In a device of the 35th inventionin a terminal unit of the 34th inventionsaid semiconductor device has the polycrystalline substance and dispersion in said electrical property of said semiconductor device originates in dispersion in a crystal structure of said polycrystalline substance.
[0048]In a device of the 36th inventionsaid code generating part is provided with OTPROM which memorizes said numerals in a terminal unit of the 33rd invention.
[0049]In a terminal unit of the 32nd thru/or the 36th one of inventions a device of the 37th inventionIn said signal transmissionfrom said wireless communication network circuithave further the 1st and 2nd mixers inserted in a course of an input signal sent to said communication circuitand said 1st mixerRestoring to an input signal which said communication circuit receivedsaid 2nd mixer modulates said input signal to which it restored using a subcarrier which has the frequency in a frequency band of said communication circuit.

[0050]A process at which a method of the 38th invention is a correspondence procedure with which entrepreneur equipment and a terminal unit of the 22nd invention communicate mutuallyand the (a) aforementioned terminal unit transmits each of said decision signal to said entrepreneur equipment(b) If conditions that each of said decision signal which received shows coincidence with each of said identification signal and said corresponding memory code are satisfiedsaid entrepreneur equipmentIf a user of said terminal unit performs attestation that he is a just user and said conditions are not satisfiedit has an attestation process which does not perform said attestation.
[0051]A process at which a method of the 39th invention is a correspondence procedure with which entrepreneur equipment and a terminal unit of the 23rd invention communicate mutuallyand the (a) aforementioned terminal unit transmits each of said identification signaland each of said memory code to said entrepreneur equipment(b) A process of judging whether it being in agreement as compared with said memory code with which said entrepreneur equipment corresponds each of said identification signal which received(c) If conditions of having judged with said entrepreneur equipment being in agreement with said memory code with which each of said identification signal corresponds in said process (b) are satisfiedIf a user of said terminal unit performs attestation that he is a just user and said conditions are not satisfiedit has an attestation process which does not perform said attestation.
[0052]A method of the 40th invention is further provided with a process on which the (e) aforementioned entrepreneur equipment records each of said identification signal which receivedand each of said memory code in a correspondence procedure of the 39th invention.
[0053]A method of the 41st invention is a correspondence procedure of the 39th inventionand in said process (c)said entrepreneur equipment records each of said identification signal which receivedand each of said memory codewhen not performing said attestation.
[0054]A process which a method of the 42nd invention acquires said identification signal of a terminal unit of the 24th invention of (a) entrepreneur equipmentand is memorized as the 1st registration code(b) A process which said entrepreneur equipment obtains said memory code of said terminal unitand memorizes as the 2nd registration code(c) After said process (a) and (b)said entrepreneur equipment and said terminal unit are provided with a communicating process which communicates mutuallyand it the communicating process (c) concerned(c-1) The 1st communicating process performed when said body part is not equipped with said auxiliary section(c-2) Have the 2nd communicating process performed when said body part is equipped with said auxiliary sectionand said 1st communicating process (c-1)(c-1-1) A process at which said terminal unit transmits said identification signal to said entrepreneur equipment(c-1-2) A process of judging whether said entrepreneur equipment comparing said received identification signal with said 1st registration codeand these

both sides being in agreement(c-1-3) If conditions that said entrepreneur equipment judged with said both sides being in agreement at said process (c-1-2) are satisfieda user of said terminal unit will perform attestation that he is a just user and said conditions will not be satisfiedit has an attestation process which does not perform said attestationA process at whichas for said 2nd communicating process (c-2)said (c-2-1) terminal unit transmits said identification signal and said memory code to said entrepreneur equipment(c-2-2) While judging whether said entrepreneur equipment compares said received identification signal with said 1st registration codeand these both sides are in agreementA process of judging whether said received memory code being compared with said 2nd registration codeand these both sides being in agreement(c-2-3) If conditions that a judgment that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-2-2) was obtained are satisfiedIf a user of said terminal unit performs high-ranking attestation that he is a just user and said conditions are not satisfiedit has a high rank attestation process of not performing said high-ranking attestation.

[0055]A method of the 43rd invention is a correspondence procedure of the 42nd invention and in said process (b)where said body part is equipped with said auxiliary sectionwhen said entrepreneur equipment and said terminal unit communicateentrepreneur equipment obtains said memory code of said terminal unit.

[0056]In a correspondence procedure of the 42nd or the 43rd invention with a method of the 44th inventionSaid process (c) is performed when said body part is equipped with said (c-3) auxiliary sectionand it is further provided with a change process of changing said 2nd registration codeand it said change process (c-3)(c-3-1) Said terminal unit with a requirement signal expressing volition of said change. While judging whether a process of transmitting said identification signal and said memory code to said entrepreneur equipmentand said identification signal which said (c-3-2) entrepreneur equipment received are compared with said 1st registration codeand these both sides are in agreementA process of judging whether said received memory code being compared with said 2nd registration codeand these both sides being in agreement(c-3-3) A process to which said change is permitted whenever it obtained a decision result that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-3-2)(c-3-4) A process of exchanging said auxiliary section of said terminal unitand equipping with an auxiliary section after exchange after said process (c-3-3) to said body partand said (c-3-5) terminal unit after said process (c-3-4)A process of transmitting said identification signal and said memory code after change based on said auxiliary section after exchange to said entrepreneur equipment(c-3-6) Said entrepreneur equipment is provided with a process of updating said 2nd registration code with said memory code after change received only within a case where said change is permittedat said process (c-3-3).

[0057]A process which a method of the 45th invention obtains said identification signal and said 1st key of a terminal unit to the 25th invention of (a) entrepreneur

equipmentand is memorized as the 1st registration code and a registration keyrespectively(b) A process which said entrepreneur equipment obtains said memory code enciphered with said 2nd key of said terminal unitand memorizes as the 2nd registration code(c) After said process (a) and (b)said entrepreneur equipment and said terminal unit are provided with a communicating process which communicates mutuallyand it the communicating process (c) concerned(c-1) The 1st communicating process performed when said body part is not equipped with said auxiliary section(c-2) Have the 2nd communicating process performed when said body part is equipped with said auxiliary sectionand said 1st communicating process (c-1)(c-1-1) Said terminal unit in form enciphered in said 1st enciphering circuit. A process of transmitting said identification signal to said entrepreneur equipmentand after said (c-1-2) entrepreneur equipment decrypts said received identification signal based on said registration keyIf a process of judging whether these both sides being in agreementand conditions that said (c-1-3) entrepreneur equipment judged with said both sides being in agreement at said process (c-1-2) are satisfied as compared with said 1st registration codeIf a user of said terminal unit performs attestation that he is a just user and said conditions are not satisfiedhave an attestation process which does not perform said attestation and said 2nd communicating process (c-2)(c-2-1) Said terminal unit in form enciphered in said 1st enciphering circuit. A process of transmitting said identification signal and a memory code to said entrepreneur equipmentand after said (c-2-2) entrepreneur equipment decrypts said received identification signal based on said registration keyWhile judging whether these both sides are in agreement as compared with said 1st registration codeA process of judging whether these both sides being in agreement as compared with said 2nd registration code after decrypting said received memory code based on said registration key(c-2-3) If conditions that a judgment that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-2-2) was obtained are satisfiedIf a user of said terminal unit performs high-ranking attestation that he is a just user and said conditions are not satisfiedit has a high rank attestation process of not performing said high-ranking attestation.

[0058]A method of the 46th invention is a correspondence procedure of the 45th inventionand in said process (b)where said body part is equipped with said auxiliary sectionwhen said entrepreneur equipment and said terminal unit communicateentrepreneur equipment obtains said memory code enciphered with said 2nd key of said terminal unit.

[0059]In a correspondence procedure of the 45th or the 46th invention with a method of the 47th inventionSaid process (c) is performed when said body part is equipped with said (c-3) auxiliary sectionand it is further provided with a change process of changing said 2nd registration codeand it said change process (c-3)(c-3-1) Said terminal unit with a requirement signal expressing volition of said change. After a process of transmitting said identification signal and said memory code to said

entrepreneur equipmentand said (c-3-2) entrepreneur equipment decrypt said received identification signal in form enciphered in said 1st enciphering circuit based on said registration keyWhile judging whether these both sides are in agreement as compared with said 1st registration codeA process of judging whether these both sides being in agreement as compared with said 2nd registration code after decrypting said received memory code based on said registration key(c-3-3) A process to which said change is permitted whenever it obtained a decision result that said entrepreneur equipment is in agreement also in any of two judgments of said process (c-3-2)(c-3-4) A process of exchanging said auxiliary section of said terminal unitand equipping with an auxiliary section after exchange after said process (c-3-3) to said body partand said (c-3-5) terminal unit. After said process (c-3-4)in form enciphered in said 1st enciphering circuit. A process of transmitting said identification signal and said memory code after change based on said auxiliary section after exchange to said entrepreneur equipment(c-3-6) It has a process of updating said 2nd registration codewith numerals obtained when said entrepreneur equipment decrypts said memory code after change received only within a case where said change is permittedat said process (c-3-3) based on said registration key.

[0060]A method of the 48th invention is a correspondence procedure of the 42nd thru/or the 47th one of inventionsand in said high rank attestation processsaid entrepreneur equipment records each numerals made into an object of comparison with each registration code at said process (c-2-2)when not performing said high-ranking attestation.

[0061]A method of the 49th invention is a correspondence procedure of the 42nd thru/or the 48th one of inventionsand in said high rank attestation processsaid entrepreneur equipment is recorded as what was able to support telex rate gold to communication before itwhen performing said high-ranking attestation.

[0062]A method of the 50th invention is a correspondence procedure of the 42nd thru/or the 49th one of inventionsand in said high rank attestation process said entrepreneur equipmentWhen performing said high-ranking attestationit records having performed the high-ranking attestation concernedand in said attestation processsaid entrepreneur equipment performs said attestation by making to record having performed said high-ranking attestation into further conditions.

[0063]A method of the 51st invention is a correspondence procedure of the 42nd thru/or the 50th one of inventionsand in said high rank attestation process said entrepreneur equipmentIn recording as that in which a commercial transaction performed by communication before it was materialized when said high-ranking attestation was performed and not performing said high-ranking attestationit records as that in which said commercial transaction performed by communication before it was not materialized.

[0064]A method of the 52nd invention is a correspondence procedure of the 38th thru/or the 51st one of inventionsand in said attestation processsaid entrepreneur

equipment continues said communicationwhen performing said attestationand when not performing said attestationit stops said communication.
[0065]In space through which a crowd who carries a terminal unit in which radio which a method of the 53rd invention is a correspondence procedure and carried communication enterprise equipment and formation of a wireless communication network which does not carry said communication enterprise equipment are possible gathers thru/or passesEven if a field which cannot perform said radio which carried said communication enterprise equipment by forming said wireless communication network between said terminal units which two or more [in said crowd / at least some] carry is in said spacecommunication of said terminal units in inside of said space is enabled.
[0066]In a correspondence procedure of the 53rd inventionsaid some of two or more terminal units which form said wireless communication network a method of the 54th invention by performing said radio which carried said communication enterprise equipmentSaid some of two or more of other terminal units which form said wireless communication network make it possible to also perform communication which carried said wireless communication network and carried said communication enterprise equipment further.
[0067]In a correspondence procedure of the 53rd or the 54th invention with a method of the 55th inventionThey are said at least some of two or more terminal units which form said wireless communication networkA terminal unit of a lot which carries said wireless communication network and communicates mutually computes a common key by exchanging mutually numerals which identify eachand exchanges signal transmission in form enciphered based on the common key concerned.
[0068]A method of the 56th invention enables communication which carried said wireless communication network only within urgent emergency traffic in a correspondence procedure of a description at the 53rd thru/or the 55th either.
[0069]In a correspondence procedure given in the 53rd thru/or the 56th either a method of the 57th inventionIt installs in said field which cannot perform said radio which carried said communication enterprise equipment for another terminal unit which can form said wireless communication networkand therebyeven when density of said crowd who carries said terminal unit is lowformation of said wireless communication network is enabled.
[0070]
[Embodiment of the Invention]Firstthe term used on these Descriptions is explained. In this Descriptionabout numeralsit is not limited to full match but the approximation within the limits defined beforehand is also included with "coincidence."
[0071][1. embodiment 1] By Embodiment 1by making another side memorize an identification signal peculiar to one side of two semiconductor substrates explains the semiconductor device which prevents the unauthorized use performed by exchanging a semiconductor substrateand the terminal unit as the applied machine.

[0072][1.1. semiconductor device] Drawing 1 is a block diagram showing the composition of the semiconductor device by Embodiment 1. This semiconductor device 600 is provided with the code generating part 400the comparison circuit 403the prescribed circuit 405and the memory 601. The code generating part 400the comparison circuit 403and the prescribed circuit 405 are formed in semiconductor substrate CH1and the memory 601 is formed in semiconductor substrate CH2 [another]. Semiconductor substrate CH1 and CH2 may be any of a gestalt and a bare chip by which the mold was carried outand they are carried on the single or multiple circuit board.

[0073]The code generating part 400 generates the identification signal Cd peculiar to semiconductor substrate CH1. The memory 601 memorizes the identification signal Cd which the code generating part 400 generated as the memory code Co. It is transmitted to the memory 601 from the code generating part 400and the identification signal Cd is written in the memory 601when the semiconductor device 600 is shipped as a product.

[0074]The comparison circuit 403 compares the identification signal Cd which the code generating part 400 generates with the memory code Co read from the memory 601judges whether these both sides are mutually in agreementand outputs the decision signal En expressing the result. As a judgment of conformityif it has a comparator of conventionally well-known which judges whether the difference of both numerals will be zero if full match nature is judgedit is sufficient for the comparison circuit 403. If the approximation nature within the limits defined beforehand is judgedthe comparison circuit 403 should just compare the size of the difference of both numerals with a fixed reference value. For examplethe size of a difference can be evaluated by the size of the difference as a numerical valueor the number of bits which is mutually different. It is also possible to constitute the semiconductor device 600 so that the input of a reference value may be enabled from the exterior and the user of the semiconductor device 600 can set a reference value as a desired value.

[0075]The prescribed circuit 405 is a circuit formed of two or more circuit elements so that it may achieve a predetermined functionand it contains the circuit part which is operation or un-operating selectively based on the decision signal En which the comparison circuit 403 outputs. The communication circuit 907 shown in drawing 65 can serve as an example of the prescribed circuit 405.

[0076]Since the semiconductor device 600 is constituted as mentioned aboveonly when the identification signal Cd which the code generating part 400 generatesand the memory code Co read from the memory 601 are mutually in agreementall the portions of the prescribed circuit 405 operate. therefore -- responding to the result of comparison by making the prescribed circuit 405 into the part of the circuit which realizes the function of an applied machine -- predetermined operation of an applied machine -- permission -- and disapproval can be carried out. Since the identification signal Cd and the memory code Co are not in agreement even if the semiconductor

substrate CH1 or CH2 tends to be exchanged to another semiconductor substrate and it is going to use an applied machine unjustlythe applied machine cannot operate predetermined. The applied machine with which the semiconductor device 600 was incorporated can be carried out in this wayand can prevent the unauthorized use by exchange of a semiconductor substrate.

[0077]The code generating part 400 and the comparison circuit 403 may be formed in single semiconductor substrate CH3and the prescribed circuit 405 may be formed in semiconductor substrate with another it. Howeverthe prescribed circuit 405 cannot input from the outside the decision signal En inputted into the prescribed circuit 405 from the comparison circuit 403 in the gestalt formed in single semiconductor substrate CH1 with the code generating part 400 and the comparison circuit 403. For this reasonthe advantage that the barrier to an unauthorized use is raised further is acquired.

[0078]The comparison circuit 403 may be formed in a semiconductor substrate other than the semiconductor substrate in which the code generating part 400 is formed. Howeverthe comparison circuit 403 cannot change unjustly the identification signal Cd inputted into the comparison circuit 403 from the code generating part 400 from the outside in the gestalt formed in the single semiconductor substrate CH1 or CH3 with the code generating part 400. For this reasonthe advantage that the barrier to an unauthorized use is raised further is acquired.

[0079]The semiconductor device 600 is possible also for carrying out the gestalt which is not provided with the prescribed circuit 405. In this caseit is good to form the prescribed circuit 405 in an applied machine separately [the semiconductor device 600]. Or it is also possible to constitute an applied machine so that the decision signal En may be taken out to the exterior of an applied machine and it can direct operation of an applied machineand un-operating from the exterior according to the value. The terminal unit of Embodiment 3 mentioned later is an example of such an applied machine.

[0080]The semiconductor device 600 is possible also for carrying out the gestalt which is not provided with the prescribed circuit 405 or the comparison circuit 403. In this caseit is good to form separately [the semiconductor device 600] the prescribed circuit 405 and the comparison circuit 403 in an applied machine. Or it is also possible to constitute an applied machine so that the identification signal Cd and the memory code Co may be taken out to the exterior of an applied machine and it can direct operation of an applied machineand un-operating from the exterior according to the value. The terminal unit of Embodiment 4 mentioned later is an example of such an applied machine.

[0081][1.2. code generating part] Drawing 2 is a block diagram showing a desirable example of the internal configuration of the code generating part 400. The code generating part 400 is provided with the semiconductor device 401 and the coding circuit 402 in the example of drawing 2. The coding circuit 402 reads the electrical

property of the semiconductor device 401 as the analog signal Anand changes it into a digital signal. The digital signal obtained by conversion is outputted as the identification signal Cd.

[0082]As an electrical property of the semiconductor device 401the characteristic which had dispersion for every individual of the semiconductor device 401 is chosen. By that causesince the identification signal Cd is generated as a value which varied for every individual of the semiconductor device 401it will be provided with the character as an identification signal peculiar to the semiconductor substrate in which the code generating part 400 is formed. Since the semiconductor device 401 manufactured at the same process can be used between the semiconductor devices 600 of a large number mass-producedmanufacture of the semiconductor device 600 can be simplified. Since the electrical property of the semiconductor device 401 which becomes a basis of the identification signal Cd cannot be changed from the outsidethe advantage that the barrier to an unjust change of the identification signal Cd is expensive is also acquired.

[0083]It is possible to use the characteristic that the semiconductor device 401 is provided with the polycrystalline substanceoriginates in dispersion in the crystal structureand varies as an electrical property. This example is explained in full detail by the following drawing 3 - drawing 6. It is also possible to use dispersion in the threshold which the semiconductor device 401 is provided with MOSFET and originates in dispersion in the impurity concentration of the impurity diffused layer.

[0084]Drawing 3 is a top view showing a desirable example of the semiconductor device 401. Drawing 4 is the sectional view which met the A-A cutout line of drawing 3. In this examplethe semiconductor device 401 has the thin film transistor (it is hereafter written as TFT) 101andmoreoverthe semiconductor layer 1060 including those channel regions is formed as the polycrystalline substance. Although the semiconductor layer 1 formed as an intermediate product in the manufacturing process of the semiconductor device 401 for the facilities of explanation is drawn on drawing 3By performing selective etching in a manufacturing processthe semiconductor layer 1 is molded by the semiconductor device 401 as a finished product to the semiconductor layer 1060.

[0085]In TFT101the gate electrode 11 is selectively formed on the insulator layer 12and the whole surface of the insulator layer 12 and the gate electrode 11 is covered with the insulator layer 10. The semiconductor layer 1 is formed on the insulator layer 10. When an example of the material of each element is describedthe insulator layer 12 is a silicon oxidethe gate electrode 11 is the polysilicon in which the impurity was dopedthe insulator layers 10 are silicon oxidessuch as TEOSand the main ingredients of the semiconductor layer 1 are silicon.

[0086]The channel regions 2 located in the upper part of the gate electrode 11the source region 3 which faces across these channel regions 2and the drain area 4 are formed in the semiconductor layer 1. The portion of the insulator layer 10 which

touches the channel regions 2 functions as gate dielectric film. In the example of drawing 3 and drawing 5the conductivity type of the channel regions 2 is a n typeand the conductivity type of the source region 3 and the drain area 4 is a p type. That isTFT101 is formed as p channel type MOS type TFT as an example. Needless to sayTFT101 may be formed as n channel type MOS type TFT.

[0087]The semiconductor layer 1 is formed as a polycrystalline semiconductor layerand as drawing 3 showsit includes the countless crystal grain (grain) 5 and the grain boundary (grain boundary) 6 which is the portions which were located in those interfaces and have produced disorder of a crystal. Although crystal orientation is uniform in the single crystal grain 5generally between the different crystal grains 5crystal orientation differs. It is randomand the size of the crystal grain 5 and arrangement are the processes in which the semiconductor layer 1 is formedand vary variously. That iseven if much TFT101 are manufactured through the same manufacturing processthe crystal structure of the semiconductor layer 1 becomes a different thing every individual of TFT101.

[0088]As a resultanother individual which should express one individual temporarily and was produced by the same manufacturing process as this in TFT101 is set to TFT102 so that it may illustrate to drawing 5If it distinguishes from TFT101the quantity of the grain boundary 6 which occupies the channel regions 2 does not become the same between TFT101 and TFT102. Drawing 5 shows the example in which the direction of TFT102 includes the grain boundary 6 few in the channel regions 2 rather than the semiconductor device 101.

[0089]It is known for the polycrystal TFT with the quantity of the grain boundary 6 included in the channel regions 2 that the characteristic varies. This fact is indicated to IEEE Transactions onElectron DevicesVol. 45No1January (1998)and pp.165-172 (followingdocument 3)for example. Namelyas the relation between the gate voltage Vg and the drain current Id is shown in drawing 6 about TFT101 and 102by TFT101 included mostlythe grain boundary 6 to the channel regions 2. Compared with TFT102 which includes the grain boundary 6 fewthe drain current Id under the gate voltage Vg0 [same] becomes small (namelyIda<Idb).

[0090]Thereforeit becomes possible to use for discernment of a semiconductor substrate dispersion in the crystal structure of the polycrystalline substance which TFT101 has. Since it originates in dispersion in the crystal structure of the polycrystalline substanceunlike the identification number recorded on the flash memory 908 (drawing 65)a different electrical property between individuals cannot be rewritten from the outside. Thereforethe security to the illegal use of an applied machine can be raised.

[0091]And the time and effort which programs to the flash memory 908 unlike the art which programs an identification number is not needed. Since the characteristic which is different for every individual unlike the art which records an identification number on a mask ROM is obtained through the same manufacturing processa manufacturing

process is simple and a production man hour and a manufacturing cost are held down low. It is largeand dispersion in the crystal structure of the polycrystalline substance originates in itand its dispersion in an electrical property is also large. For this reasonit is possible to secure the width of dispersion in the identification signal Cd widely. That isit is easy to keep an identification signal from being mutually in agreement between the semiconductor devices 600 of a large number mass-produced.

[0092]Although a manufacturing process becomes complicatedonly the channel regions 2 of TFT101 may be formed with a polycrystalline semiconductorthe source region 3 and the drain area 4 may be formed with the single crystal semiconductorand the characteristic varies at random in a similar manner even in this case.

[0093]It is also possible to changethough the electrical property of the semiconductor device 401 shown in drawing 2 - drawing 6 is minute in connection with change of temperature and time. The identification signal Cd always not holding a fixed value in a perfect meaningand being accompanied by a certain amount of change in connection with itis also assumed. In order to cope with thisthe comparison circuit 403 is in the tolerance level also in consideration of change of the identification signal Cdand is good to judge the conformity of numerals.

[0094]As an example which the semiconductor device 401 equips with the polycrystalline substanceit is possible not only TFT shown in drawing 3 - drawing 6 but to carry out the example of other elementssuch as a resistance element provided with the polycrystalline substance and a capacitative element provided with the polycrystalline substance. The semiconductor device 401 may be provided with two or more TFT(s) etc. The width of dispersion in the identification signal Cd is expandedso that there is much numbersuch as TFT. In Embodiment 12these examples are explained in detail.

[0095][Example using 1.3. OTPROM] Drawing 7 is a block diagram showing another desirable example of the internal configuration of the code generating part 400. The code generating part 400 is provided with OTP(One Time Programable) ROM602 which is the nonvolatile memory which can be restricted at once and can be written in in the example of drawing 7. When the semiconductor device 600 is shippedthe identification signal Cd is written in OTPROM602. Thenafter the semiconductor device 600 includes a user's handit is technically impossible to rewrite the identification signal Cd currently written in OTPROM602. That isalso in the example of drawing 7the advantage that the technical barrier to an unjust change of the identification signal Cd which the code generating part 400 generates is expensive is acquired.

[0096]OTPROM is suitable also for use in the memory 601as not only the code generating part 400 but drawing 8 shows. The memory 601 is provided with OTPROM602 in the example of drawing 8. When the semiconductor device 600 is shippedthe identification signal Cd transmitted from the code generating part 400 is written in OTPROM602 with which the memory 601 is equipped as the memory code

Co. Thenafter the semiconductor device 600 includes a user's handit is technically impossible to rewrite the memory code Co currently written in OTPROM602. That isin the example of drawing 8the advantage that the technical barrier to an unjust change of the mernory code Co memorized by the memory 601 is expensive is acquired. The semiconductor substrate in which the code generating part 400 was formed can be exchanged by that causeand the unauthorized use performed by rewriting the memory code Co memorized by the memory 601 simultaneously with it so that it may be in agreement with the identification signal Cd of a new semiconductor substrate can also be prevented.

[0097][1.4. terminal unit] Drawing 9 is a block diagram showing the composition of the terminal unit as an applied machine of the semiconductor device 600. This terminal unit 1001 is constituted as a portable telephone. The semiconductor device 1002 with which the terminal unit 1001 is provided is an example of the semiconductor device 600 shown in drawing 1and is provided with the communication circuit 405a as the prescribed circuit 405.

[0098]Preferablyalthough the code generating part 400the comparison circuit 403and the comrnunication circuit 405a are formed in single semiconductor substrate CH100Only the comparison circuit 403 and the code generating part 400 may be formed in single semiconductor substrate CH102and only the code generating part 400 may be formed in a single semiconductor substrate. Even if it is which casethe memory 654 which memorizes the memory code Co is formed in different semiconductor substrate CH51 from the semiconductor substrate in which the code generating part 400 is formed.

[0099]The communication enterprise (it is written as "office" if needed) equipment 655 which is equipment of the entrepreneur who carries communication of the terminal unit 1001 is equipped with the communication circuit 656. Between the communication circuit 405a and the communication circuit 656the signal transmission which makes a sounddataetc. the contents is exchanged considering radio (namelyelectric wave) as a medium. The communications system 1000 is constituted by the terminal unit 1001 and the communication enterprise equipment 655.

[0100]Drawing 10 is a block diagram showing an example of the internal configuration of the communication circuit 405a. In the communication circuit 405a with which the terminal unit 1001 which carries radio is providedthe well-known radio frequency circuit 462 and the intermediate frequency circuit 463 intervene between an antenna and the digital disposal circuit (baseband circuit) 800. The sending circuit 460 and the receiving circuit 461 are equippedit is received by the receiving circuit 461 and the signal transmission Dt is transmitted to the digital disposal circuit 800 by the sending circuit 406.

[0101]In the example of drawing 10only the sending circuit 460 is turned on and off with the decision signal En. That isthe comparison circuit's 403 judgment of the disagreement of numerals will stop a transmitting function. It is also possible to

constitute the communication circuit 405 so that it may be accepted receiving-circuit 461 or the both sides of the sending circuit 460 and the receiving circuit 461 may turn on and off based on the decision signal En.

[0102]Drawing 11 is a flow chart which shows the flow of processing until the terminal unit 1001 is appropriated for the use to communication. Firstthe semiconductor device 600 (specifically semiconductor device 1001) as parts is manufactured (S201). The identification signal Cd is recorded on the memory 601 as the memory code Co before the final process thru/or it (S202). Thenthe semiconductor device 600 is supplied to a telephone maker and the terminal unit 1001 is assembled by the telephone maker (S203). After user(user)-passing through the completed terminal unit 1001 and supplying it (S204)it is appropriated for the use to communication by a user (S205).

[0103]Steps S206-S210 express the communicative procedurei.e.the internal flow of Step S205in which the terminal unit 1001 was used. If communication is startedthe terminal unit 1001 will read the memory code Co from the memory 601 (S206). Nextcomparison with the identification signal Cd and the memory code Co is performed by the comparison circuit 403and the decision signal En expressing the decision result about whether both sides are in agreement is generated (S207).

[0104]When the decision signal En shows coincidence of numerals(S208) and the communication circuit 405a continue communications processing by maintaining a communication function (S209). On the other handwhen the decision signal En shows the disagreement of numerals(S208) and the communication circuit 405a communicate impossible by suspending either [at least] a transmitting function or a receiving function (S210). Processing will be ended if communication is completed.

[0105]As mentioned abovein the terminal unit 1001when the decision signal En shows the disagreement of numerals. It is automatically stopped by work of terminal unit 1001 itselfwithout the malfeasance of exchanging a semiconductor substrate and using it for communication waiting for processing by the communication enterprise equipment 655since the function of at least a part of communication circuit 405a stops.

[0106]Although the portable telephone which makes radio communication media as a terminal unit was made into the example in the above explanationthis embodiment is applicable similarly to the telephone of the cable which makes a telecommunication cable communication media. It is applicable also not only to telephone but various terminal units.

[0107]Drawing 12 has illustrated various terminal units which can apply this embodimentand the entrepreneur equipment (server) which a terminal unit makes a communicative object. For exampleit may be a terminal unit in the end of an automatic car end it communicates with the highway managerial system which manages the payment of the usage fee of a highwayetc. automaticallyand it may be the IC card or personal computer which communicates with the ATM system of a

bank and performs the drawerdepositetc. of cash.
[0108][2. embodiment 2] By Embodiment 2the number of the semiconductor substrate identified with a peculiar identification signal explains the gestalt extended from the singular number to plurality in the semiconductor device and terminal unit of Embodiment 1.
[0109]Drawing 13 is a block diagram showing the composition of the semiconductor device by Embodiment 2. In the semiconductor device 620 which drawing 13 showsthe memory 601 other than the code generating part 400the comparison circuit 403and the prescribed circuit 405 is formed in semiconductor substrate CH4and the code generating part 400 and the comparison circuit 403 other than the memory 601 are formed in semiconductor substrate CH5 [another]. The code generating part 400 which the code generating part 400 formed in semiconductor substrate CH4 generated identification signal Cd1 [peculiar to semiconductor substrate CH4]and was formed in semiconductor substrate CH5 generates identification signal Cd2 [peculiar to semiconductor substrate CH5].
[0110]The memory 601 formed in semiconductor substrate CH4The memory 601 which memorized identification signal Cd2 transmitted from the code generating part 400 formed in semiconductor substrate CH5 as memory code Co2and was formed in semiconductor substrate CH5Identification signal Cd1 transmitted from the code generating part 400 formed in semiconductor substrate CH4 is memorized as memory code Co1. That isthe identification signal Cd peculiar to two eachsemiconductor substrate CH4 and CH5and Cd2 are memorized by the memory 601 formed in the semiconductor substrate of another side.
[0111]The comparison circuit 403 formed in semiconductor substrate CH4 compares identification signal Cd1 with memory code Co1and the comparison circuit 403 formed in semiconductor substrate CH5 compares identification signal Cd2 with memory code Co2. The prescribed circuit 405 formed in semiconductor substrate CH4 contains the circuit part which is operation or un-operating selectively based on the group of decision signal En1 which the two comparison circuits 403 outputand En2. For example in the communication circuit 405a of drawing 10when Eneither one of decision signal En1 or 2 shows the disagreement of numeralsthe prescribed circuit 405 can constitute the sending circuit 560 so that operation may be suspended. It becomes possible to raise further the barrier to the unauthorized use by exchange of a semiconductor substrate by it.
[0112]It is also possible to extend the number of the semiconductor substrate to which the peculiar identification signal Cd is given to three or more pieces. For examplethey are formed in each of three semiconductor substrates by the code generating part 400 and the memory 601 which generate the peculiar identification signal Cdand the memory 601A semiconductor device may be constituted so that the identification signal Cd transmitted from the code generating part 400 formed in the semiconductor substrate other than the semiconductor substrate in which itself is

formed may be memorized. Or at least a part of three memories 601 may be formed in a semiconductor substrate other than three semiconductor substrates in which the code generating part 400 is formed.

[0113]The barrier to the unauthorized use of an applied machine can be raised moreso that there is much number of the semiconductor substrate to which the identification signal Cd was giveni.e.a semiconductor substrate provided with the code generating part 400. The number of a semiconductor substrate can be held down to the minimum by forming the memory 601 only in a semiconductor substrate provided with the code generating part 400. Especially in the semiconductor device 620 shown in drawing 13the advantage that the barrier to an unauthorized use can be raised is acquiredsuppressing the number of a semiconductor substrate to two pieces equivalent to the number of the semiconductor substrate in the semiconductor device 600 shown in drawing 1.

[0114]Drawing 14 is a block diagram showing the composition of the terminal unit as an applied machine of the semiconductor device 620. This terminal unit 1011 is constituted as a portable telephoneand constitutes the communications system 1010 with the communication enterprise equipment 655. The semiconductor device 1012 with which the terminal unit 1011 is provided is an example of the semiconductor device 620 shown in drawing 13and is provided with the communication circuit 405a as the prescribed circuit 405. The communication circuit 405a suspends a part of the functionswhen Eneither decision signal En1 or 2 shows the disagreement of numerals.

[0115]Although the memory 601 and the communication circuit 405a which memorize preferably the code generating part 400 which generates identification signal Cd1the comparison circuit 403 which makes identification signal Cd1 a comparison objectand memory code Co2 are formed in single semiconductor substrate CH103Only the comparison circuit 403the memory 601and the code generating part 400 may be formed in single semiconductor substrate CH11and only the code generating part 400 may be formed in single semiconductor substrate CH104. The memory 601 which memorizes memory code Co1 is preferably formed in single semiconductor substrate CH13 with the code generating part 400 which generates identification signal Cd2and the comparison circuit 403 made into the object of comparison of identification signal Cd2.

[0116]Drawing 15 is a flow chart which shows the flow of processing until the terminal unit 1011 is appropriated for the use to communication. Firstthe semiconductor device 620 (specifically semiconductor device 1012) as parts is manufactured (S241). Identification signal Cd1 of each semiconductor substrate and Cd2 are recorded on the memory 601 of the semiconductor substrate of another side as memory code Co1 and Co2 before the final process thru/or it (S242). Thenthe semiconductor device 620 is supplied to a telephone maker and the terminal unit 1011 is assembled by the telephone maker (S243). After the completed terminal unit 1011 is supplied to a user (S244)it is appropriated for the use to communication by a user (S245).

[0117]Steps S246-S250 express the communicative procedurei.e.the internal flow of Step S245in which the terminal unit 1011 was used. If communication is startedthe terminal urit 1011 will read the memory codes Co1 and Co2 from the two memories 601 (S246). At the same time decision signal En1 expressing the decision result about whether comparison with identification signal Cd1 and memory code Co1 is performed by one comparison circuit 403and next both sides are in agreement by it is outputted by the comparison circuit 403 of another side. Comparison with identification signal Cd2 and memory code Co2 is performedand decision signal En2 expressing the decision result about whether both sides are in agreement is outputted (S247).
[0118]both decision signal En1 and En2 -- although -- when coincidence of numerals is shown(S248) and the communication circuit 405a continue communications processing by maintaining a communication function (S249). On the other handwhen Eneither decision signal En1 or 2 shows the disagreement of numerals(S248) and the communication circuit 405a communicate impossible by suspending either [at least] a transmitting function or a receiving function (S250). Processing will be ended if communication is completed.
[0119][3. embodiment 3] Embodiment 3 explains the terminal unit which used the portion except a prescribed circuit in the semiconductor device by Embodiment 1 or 2.
[0120]Drawing 16 is a block diagram showing the composition of the terminal unit by Embodiment 3. As for this terminal unit 1001the communication circuit 405a does not perform operation or un-operating selectively based on the decision signal En sent from the comparison circuit 403In the point which only transmits the decision signal En to the communication enterprise equipment 655 as a part of signal transmissionit differs characteristic [the terminal unit 1001 of Embodiment 1 shown in drawing 9].
[0121]The flow of processing is drawn on a par with the flow chart of drawing 11 until the terminal unit 1001 of drawing 16 is appropriated for the use to communication. Howeverthe internal flow of Step S205 is transposed to processing of Step S1000 of drawing 17. If processing of Step S1000 is startedthe terminal unit 1001 will read the memory code Co from the memory 601 (S206). Nextcomparison with the identification signal Cd and the memory code Co is performed by the comparison circuit 403and the decision signal En expressing the decision result about whether both sides are in agreement is generated (S207).
[0122]This decision signal En is transmitted to the communication enterprise equipment 655 through the communication circuit 405a (S208S1001S1003). In other wordswhen the decision signal En shows coincidence of numeralsthe predetermined value which shows coincidence of numerals as (S208) and the decision signal En is transmitted (S1001)and when the decision signal En shows the disagreement of numerals(S208) and the above-mentioned predetermined value are not transmitted (S1003).
[0123]The communication enterprise equipment 655 does not attestwhen attestation that the user of the terminal unit 1001 is a just user when the decision signal En

shows coincidence of numerals is performed and the decision signal En shows the disagreement of numerals. The communication enterprise equipment 655 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S1002)and not attesting (S1004).

[0124]Thusin the terminal unit 1001 of drawing 16the judgment source of the authenticating processing performed by the communication enterprise equipment 655 side can be presented with the decision signal Entherebyit can eliminate from the object of attestation of the unauthorized use by exchange of a semiconductor substrateand high-precision attestation can be realized. Permission or disapproval of a commercial transactionetc. can perform offer of a certain serviceor un-providing as processing accompanying authenticating processing in addition to communicative continuation or stop. Or processing in which the judgment source of attestation is only recorded may be performed. A next embodiment explains these examples.

[0125]Drawing 18 is a block diagram showing another example of composition of the terminal unit by Embodiment 3. As for this terminal unit 10011the communication circuit 405a does not perform operation or un-operating selectively based on decision signal En1 sent from the comparison circuit 403and En2In the point which only transmits decision signal En1 and En2 to the communication enterprise equipment 655 as a part of signal transmissionit differs characteristic [the terminal unit 1011 of Embodiment 1 shown in drawing 14].

[0126]The flow of processing is drawn on a par with the flow chart of drawing 15 until the terminal unit 1011 of drawing 18 is appropriated for the use to communication. Howeverthe internal flow of Step S245 is transposed to processing of Step S1010 of drawing 19. If processing of Step S1010 is startedthe terminal unit 1011 will read memory code Co1 and Co2 from the two memories 601 (S246). Nextcomparison with identification signal Cd1 and memory code Co1 is performed by one comparison circuit 403and decision signal En1 expressing the decision result about whether both sides are in agreement is generated. comparison with identification signal Cd2 and memory code Co2 is performed by itsimultaneously the comparison circuit 403 of another sideand decision signal En2 expressing the decision result about whether both sides are in agreement is generated. (S247).

[0127]These decision signal En1 and En2 are transmitted to the communication enterprise equipment 655 through the communication circuit 405a (S248S1001S1003). if it puts in another way -- both decision signal En1 and En2 -- although -- the time of coincidence of numerals being shown -- (S248). The predetermined value which shows coincidence of numerals as decision signal En1 and En2 is transmitted (S1001)and when Eneither decision signal En1 or 2 shows the disagreement of numerals(S208) and the above-mentioned predetermined value are not transmitted (S1003).

[0128]the communication enterprise equipment 655 -- both decision signal En1 and

En2 -- although -- when attestation that the user of the terminal unit 1001 is a just user when coincidence of numerals is shown is performed and Eneither decision signal En1 or 2 shows the disagreement of numeralsit does not attest. The communication enterprise equipment 655 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S1002)and not attesting (S1004).

[0129]Thusin the terminal unit 1001 of drawing 18the judgment source of the authenticating processing performed by the communication enterprise equipment 655 side can be presented with decision signal En1 and En2therebyit can eliminate from the object of attestation of the unauthorized use by exchange of a semiconductor substrateand high-precision attestation can be realized. Since two decision signal En1 and En2 are made into a judgment sourcethe accuracy of attestation can be further raised rather than the terminal unit 1001 of drawing 16.

[0130][4. embodiment 4] Embodiment 4 explains the terminal unit which used the portion except the both sides of the prescribed circuit and the comparison circuit in the semiconductor device by Embodiment 1 or 2.

[0131]Drawing 20 is a block diagram showing the composition of the terminal unit by Embodiment 4. The semiconductor device 652 with which this terminal unit 801 is provided The comparison circuit 403 is removed and the communication circuits 405a differ characteristic [the semiconductor device 1002 of Embodiment 1 which showed drawing 9 the identification signal Cd and the memory code Co in the point which only transmits to the communication enterprise equipment 655 as a part of signal transmission].

[0132]In addition to the communication circuit 656the communication enterprise equipment 655 of drawing 20 is provided with the decision circuit 657 and the customer data memory 658. The communication enterprise equipment 655 and the terminal unit 801 constitute the communications system 800.

[0133]The flow of processing is drawn on a par with the flow chart of drawing 11 until the terminal unit 801 is appropriated for the use to communication.

However however the internal flow of Step S205 is transposed to processing of Step S260 of drawing 21. If processing of Step S260 is startedthe terminal unit 801 will transmit the identification signal Cd and the memory code Co to the communication enterprise equipment 655 (S261). In connection with itthe communication enterprise equipment 655 receives the identification signal Cd and the memory code Co by the communication circuit 656 (S262).

[0134]The communication enterprise equipment 655 judges whether as compared with the nextboth sides are mutually in agreement in the identification signal Cd and the memory code Co by the decision circuit 657and tells the decision signal En which shows a decision result to the communication circuit 656 (S263). The communication enterprise equipment 655 performs (S264) and attestation that the user of the terminal unit 801 is a just userwhen the decision signal En shows coincidence of

numeralsand when the decision signal En shows the disagreement of numeralsit does not perform (S264) and attestation. The communication enterprise equipment 655 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S265)and not attesting (S268).

[0135]When directions are made [recording the identification signal Cd and the memory code Co and] and it does not perform (S266) and attestationthe identification signal Cd and the memory code Co are recorded on the customer data memory 658 (S267). And after communications processing is stoppedfor example (S278)specification of (S269) and an unauthorized use person is made by comparing the identification signal Cd and the memory code Co with the contents of the customer data memory 658 recorded in the past (S270).

[0136]It is also possible to perform only record (S267) of the identification signal Cd and the memory code Cowithout stopping communications processingwhen not attesting. It is also possible to perform record (S267) of the identification signal Cd and the memory code Co regardless of an authentication result. In the case of the latterprocessing of Step S267 is performed among Steps S263 and S264for example.

[0137]Thusby the communication enterprise equipment 655 sidein the terminal unit 801 of drawing 20can present the judgment source of the authenticating processing performed with the identification signal Cd and the memory code Coand by that causeIt can eliminate from the object of attestation of the unauthorized use by exchange of a semiconductor substrateand high-precision attestation can be realized.

[0138]Drawing 22 is a block diagram showing another example of composition of the terminal unit by Embodiment 4. The semiconductor device 652 with which this terminal unit 811 is providedThe comparison circuit 403 is removed and the communication circuits 405a differ characteristic [the semiconductor device 1012 of Embodiment 1 which showed drawing 14 identification signal Cd1Cd2 and memory code Co1and Co2 in the point which only transmits to the communication enterprise equipment 655 as a part of signal transmission].

[0139]In addition to the communication circuit 656the communication enterprise equipment 655 of drawing 22 is provided with the decision circuit 657 and the customer data memory 658. The communication enterprise equipment 655 and the terminal unit 811 constitute the communications system 810.

[0140]The flow of processing is drawn on a par with the flow chart of drawing 15 until the terminal unit 811 is appropriated for the use to communication.

Howeverhoweverthe internal flow of Step S245 is transposed to processing of Step S280 of drawing 23. If processing of Step S280 is startedthe terminal unit 811 will transmit identification signal Cd1Cd2 and memory code Co1and Co2 to the communication enterprise equipment 655 (S211). In connection with itthe communication enterprise equipment 655 receives identification signal Cd1Cd2 and memory code Co1and Co2 by the communication circuit 656 (S272).

[0141]The communication enterprise equipment 655 compares identification signal Cd2 with memory code Co2and judges whether both sides are mutually in agreement while it judges whether both sides are mutually in agreement in identification signal Cd1 and memory code Co1 by the decision circuit 657 as compared with the next. And the decision signal En which shows those decision results is told to the communication circuit 656 (S273). The communication enterprise equipment 655 performs (S274) and attestation that the user of the terminal unit 811 is a just userwhen coincidence of numerals is accepted in the both sides of two comparisonand when the disagreement of numerals is accepted in either of two comparisonit does not perform (S274) and attestation. The communication enterprise equipment 655 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S275)and not attesting (S278).

[0142]When directions are made [recording identification signal Cd1Cd2 and memory code Co1and Co2 and] and it does not perform (S276) and attestationidentification signal Cd1Cd2 and memory code Co1and Co2 are recorded on the customer data memory 658 (S277). And after communications processing is stoppedfor example (S278)specification of (S279) and an unauthorized use person is made by comparing identification signal Cd1Cd2 and memory code Co1and Co2 with the contents of the customer data memory 658 recorded in the past (S280).

[0143]It is also possible to perform only record (S277) of identification signal Cd1Cd2 and memory code Co1and Co2without stopping communications processingwhen not attesting. It is also possible to perform record (S277) of identification signal Cd1Cd2 and memory code Co1and Co2 regardless of an authentication result. In the case of the latterprocessing of Step S277 is performed among Steps S273 and S274for example.

[0144]Thusby the communication enterprise equipment 655 sidein the terminal unit 811 of drawing 23can present the judgment source of the authenticating processing performed with identification signal Cd1Cd2 and memory code Co1and Co2and by that causeIt can eliminate from the object of attestation of the unauthorized use by exchange of a semiconductor substrateand high-precision attestation can be realized. Since two identification signal Cd1 and Cd2 are made into a comparative objectthe accuracy of attestation can be further raised rather than the terminal unit 801 of drawing 21.

[0145][5. embodiment 5] In the semiconductor device by Embodiment 1 or 2Embodiment 5 explains the gestalt which performs an exchange of the identification signal Cd between semiconductor substratesand the memory code Co in the enciphered form.

[0146]Drawing 24 is a block diagram showing the composition of the semiconductor device by Embodiment 5. In the semiconductor device 630 which drawing 24 showsthe enciphering circuit 631the decoding circuit 632and the key generation part 633 are

formed in the semiconductor substrate CH20 or CH22 in which the code generating part 400 is formed.

[0147]The key generation part 633 generates the key K for encryption. The key K is generated like the identification signal Cd as numerals peculiar to the semiconductor substrate CH20 or CH22. The enciphering circuit 631 enciphers the identification signal Cd which the code generating part 400 generates to identification signal Cd# based on the key K which the key generation part 633 generatesand sends it out to the memory 601 formed in semiconductor substrate CH21. The memory 601 memorizes enciphered identification signal Cd# as enciphered memory code Co#.

[0148]The decoding circuit 632 reads enciphered memory code Co# which is memorized by the memory 601decrypts it to the memory code Co based on the key K which the key generation part 633 generatesand is supplied to the comparison circuit 403. The prescribed circuit 405 contains the circuit part which is operation or un-operating based on the decision signal En which the comparison circuit 403 outputs.

[0149]As mentioned abovein the semiconductor device 630between different semiconductor substratessince the identification signal Cd and the memory code Co are exchanged in the enciphered formneither the identification signal Cd nor the memory code Co can be read in the exterior. For this reasonthe barrier to an unauthorized use is raised further.

[0150]Drawing 25 is a block diagram showing an example of the internal configuration of the key generation part 633. In the example of drawing 25the key generation part 633 is provided with OTPROM602and the key K is written in OTPROM602 at the time of shipment of the semiconductor device 630. For this reasonthe key K which the key generation part 633 generates cannot be changed unjustly. Since the key K is already written in at the time of shipment of the semiconductor device 630the key K is not revealed to a user.

[0151]Drawing 26 is a block diagram showing another example of the internal configuration of the key generation part 633. The key generation part 633 of drawing 26 is provided with the semiconductor device 401 and the coding circuit 402 which were shown in drawing 2. The coding circuit 402 reads the electrical property of the semiconductor device 401 as the analog signal Anand changes it into a digital signal. The digital signal obtained by conversion is outputted as the key K.

[0152]As an electrical property of the semiconductor device 401the characteristic which had dispersion for every individual of the semiconductor device 401 is chosen. Since the key K is generated as a value which varied for every individual of the semiconductor device 401this will be provided with the character as an identification signal peculiar to the semiconductor substrate in which the key generation part 633 is formed. It is not necessary to write in the key Kand since the semiconductor device 401 manufactured at the same process can be further used between the semiconductor devices 630 of a large number mass-producedmanufacture of the semiconductor device 630 can be simplified. Since the electrical property of the

semiconductor device 401 which becomes a basis of the key K cannot be changed from the outsidethe advantage that the barrier to an unjust change of the key K is expensive is also acquired.

[0153]As illustrated to drawing 3 – drawing 6it is possible to use the electrical property which the semiconductor device 401 is provided with the polycrystalline substanceoriginates in dispersion in the crystal structureand varies. Dispersion in the crystal structure of the polycrystalline substance is largeand it is possible to originate in itand to secure the width of dispersion in the key K widelysince dispersion in an electrical property is also large. That isit is easy to keep the key K from being mutually in agreement between the semiconductor devices 630 of a large number mass-produced.

[0154]In the terminal unit 1001 of drawing 9drawing 27 is a flow chart which shows the flow of processing until the terminal unit 1001 is appropriated for the use to communicationwhen the semiconductor device 630 of drawing 24 is used instead of the semiconductor device 1002 and the prescribed circuit 405 is made into the communication circuit 405a. Firstthe semiconductor device 630 as parts is manufactured (S301). Identification signal Cd# enciphered before the final process thru/or it is recorded on the memory 601 as memory code Co# (S302). Thenthe semiconductor device 630 is supplied to a telephone maker and the terminal unit 1001 is assembled by the telephone maker (S303). After the completed terminal unit 1001 is supplied to a user (S304)it is appropriated for the use to communication by a user (S305).

[0155]Steps S306-S310 express the communicative procedurei.e.the internal flow of Step S305in which the terminal unit 1001 was used. If communication is startedthe terminal unit 1001 will read memory code Co# from the memory 601 (S306). Nextwhen memory code Co# is decrypted by the decoding circuit 632 to the memory code Cocomparison with the identification signal Cd and the memory code Co is performed by the comparison circuit 403and the decision signal En expressing the decision result about whether both sides are in agreement is generated (S307).

[0156]When the decision signal En shows coincidence of numerals(S308) and the communication circuit 405a continue communications processing by maintaining a communication function (S309). On the other handwhen the decision signal En shows the disagreement of numerals(S308) and the communication circuit 405a communicate impossible by suspending either [at least] a transmitting function or a receiving function (S310). Processing will be ended if communication is completed.

[0157]Drawing 28 is a block diagram showing another example of composition of the semiconductor device by Embodiment 5. In the semiconductor device 620 of drawing 13the semiconductor device 635 which drawing 28 shows is constituted so that identification signal Cd1Cd2 and memory code Co1and Co2 may be exchanged in the form enciphered between two semiconductor substrates. That isthe enciphering circuit 631the decoding circuit 632and the key generation part 633 are formed in the

both sides of the two semiconductor substrates CH20 (or CH22) and CH3 in which the code generating part 400the comparison circuit 403and the memory 601 are formed.

[0158]In semiconductor substrate CH20 (or CH22)the key generation part 633 generates the key K1 peculiar to semiconductor substrate CH20 (or CH22)and the enciphering circuit 631 enciphers identification signal Cd1 to identification signal Cd1# based on the key K1and it sends it out to the memory 601 of semiconductor substrate CH23. The memory 601 of semiconductor substrate CH23 memorizes identification signal Cd1# as memory code Co1#. The decoding circuit 632 of semiconductor substrate CH20 (or CH22) reads memory code Co1# from the memory 601decrypts it to memory code Co1 based on the key K1and is supplied to the comparison circuit 403.

[0159]In semiconductor substrate CH23the key generation part 633 generates the key K2 peculiar to semiconductor substrate CH23and the enciphering circuit 631 enciphers identification signal Cd2 to identification signal Cd2# based on the key K2and it sends it out to the memory 601 of semiconductor substrate CH20 (or CH22). The memory 601 of semiconductor substrate CH20 (or CH22) memorizes identification signal Cd2# as memory code Co2#. The decoding circuit 632 of semiconductor substrate CH23 reads memory code Co2# from the memory 601decrypts it to memory code Co2 based on the key K2and is supplied to the comparison circuit 403. The prescribed circuit 405 contains the circuit part which is operation or un-operating based on the group of two decision signal En1 which the two comparison circuits 403 outputand En2.

[0160]As mentioned abovein the semiconductor device 635between different semiconductor substratessince identification signal Cd1Cd2 and memory code Co1and Co2 are exchanged in the enciphered formneither identification signal Cd1 nor Cd2 nor memory code Co1 nor Co2 can be read in the exterior. For this reasonthe barrier to an unauthorized use is raised further.Like the semiconductor device 620 (drawing 13) of Embodiment 2since two decision signal En1 and En2 are usedit becomes possible to raise further the barrier to the unauthorized use by exchange of a semiconductor substrate.

[0161]Also in the semiconductor device whose semiconductor substrate in which the code generating part 400 was formed is three or more piecesSimilarlyit is possible by arranging the enciphering circuit 631the decoding circuit 632and the key generation part 633 to each semiconductor substrate to communicate in the form which enciphered the identification signal and the memory code between different semiconductor substrates.

[0162]In the terminal unit 1011 of drawing 14drawing 29 is a flow chart which shows the flow of processing until the terminal unit 1011 is appropriated for the use to communicationwhen the semiconductor device 635 of drawing 28 is used instead of the semiconductor device 1012 and the prescribed circuit 405 is made into the

communication circuit 405a. Firstthe semiconductor device 635 as parts is manufactured (S341). Identification signal Cd1# as which each semiconductor substrate was enciphered before the final process thru/or itand Cd2# are recorded on the memory 601 of the semiconductor substrate of another side as memory code Co1# and Co2# (S342). Thenthe semiconductor device 620 is supplied to a telephone maker and the terminal unit 1011 is assembled by the telephone maker (S343). After the completed terminal unit 1011 is supplied to a user (S344)it is appropriated for the use to communication by a user (S345).

[0163]Steps S346-S350 express the communicative procedurei.e.the internal flow of Step S345in which the terminal unit 1011 was used. If communication is startedthe terminal unit 1011 will read memory code Co1# and Co2# from the two memories 601 (S346). Nextafter memory code Co1# and Co2# are decrypted by the two decoding circuits 632 memory code Co1 and Co2by one comparison circuit 403. At the same time decision signal En1 expressing the decision result about whether comparison with identification signal Cd1 and memory code Co1 is performedand both sides are in agreement is outputted by the comparison circuit 403 of another side. Comparison with identification signal Cd2 and memory code Co2 is performedand decision signal En2 expressing the decision result about whether both sides are in agreement is outputted (S347).

[0164]both decision signal En1 and En2 -- although -- when coincidence of numerals is shown(S348) and the communication circuit 405a continue communications processing by maintaining a communication function (S349). On the other handwhen Eneither decision signal En1 or 2 shows the disagreement of numerals(S348) and the communication circuit 405a communicate impossible by suspending either [at least] a transmitting function or a receiving function (S350). Processing will be ended if communication is completed.

[0165][6. embodiment 6] In the semiconductor device by Embodiment 5Embodiment 6 explains the gestalt in which the switching circuit which performs exclusively sending out of the enciphered identification signal and the input of the enciphered memory code is established.

[0166]Drawing 30 is a block diagram showing the composition of the semiconductor device by Embodiment 6. In addition to the enciphering circuit 631the decoding circuit 632and the key generation part 633the switching circuit 641 is formed in the semiconductor substrate CH40 or CH42 in which the code generating part 400 is formed in the semiconductor device 640 which drawing 30 shows. The channels of communication of identification signal Cd# sent out to the memory 601 by which the switching circuit 641 was formed in semiconductor substrate CH41 from the enciphering circuit 631And it is inserted in the channels of communication of memory code Co# sent to the decoding circuit 632 from the memory 601and transfer of identification signal Cd# and transfer of memory code Co# are performed exclusively.

[0167]So that a user may mean an unauthorized use and identification signal Cd#

which the enciphering circuit 631 outputs may be inputted into the decoding circuit 632 as it isEven if it short-circuits the terminal of semiconductor substrate CH40 (or CH42)identification signal Cd# is not inputted as it is into the decoding circuit 632 by work of the switching circuit 641. That iseven if an unauthorized use is meant by the short circuit of a terminalit cannot pretend to be the comparison circuit 403 as if the identification signal Cd and the memory code Co were in agreement. Thusthe semiconductor device 640 also prevents the unauthorized use of the applied machine made by short-circuiting the terminal of a semiconductor substrate.

[0168]Even if it inserts the switching circuit 641 between the code generating part 400 and the enciphering circuit 631 and between the comparison circuit 403 and the decoding circuit 632an effect equivalent to the semiconductor device 640 of drawing 30 is acquired. Generallythe switching circuit 641 should just be inserted in the channels of communication of the identification signal Cd (or Cd#) in which it results [from the code generating part 400] to the memory 601and the channels of communication of the memory code Co (or Co#) in which it results [from the memory 601] to the comparison circuit 403.

[0169]The switching circuit 641 is applicable also to the semiconductor device 600 of drawing 1 which is not provided with enciphering circuit 631 grade. Namelyso that it may be inserted in the channels of communication of the identification signal Cd in which it results [from the code generating part 400] to the memory 601and the channels of communication of the memory code Co in which it results [from the memory 601] to the comparison circuit 403 in the semiconductor device 600 of drawing 1It is also possible to form the switching circuit 641 in semiconductor substrate CH1 (or CH3). Therebyan effect equivalent to the semiconductor device 640 of drawing 30 is acquired.

[0170]The switching circuit 641 can also be applied to the semiconductor device 620 shown in drawing 13and the semiconductor device 635 shown in drawing 28. When applied to the semiconductor device 620 of drawing 13the switching circuit 641 is formed in the both sides of semiconductor substrate CH4 (or CH6) and semiconductor substrate CH5. When applied to the semiconductor device 635 of drawing 28the switching circuit 641 is formed in the both sides of semiconductor substrate CH20 (or CH22) and semiconductor substrate CH23.

[0171][7. embodiment 7] The key generation part 633 provided with the semiconductor device 401 explained by Embodiment 5 is applicable also to the common terminal unit which performs an exchange of a host computer and data. Embodiment 7 explains the terminal unit constituted such.

[0172]Drawing 31 is a block diagram showing the composition of the terminal unit by Embodiment 7. The terminal unit 821 and the host computer 825 connected to this constitute the system 820 which exchanges the data Dd of each other. In addition to the data input part 822 which inputs the data Ddand the data output part 823 which outputs the data Ddthe terminal unit 821 is provided with the enciphering circuit

631the decoding circuit 632and the key generation part 633. The key generation part 633 generates the key K for encryption. The enciphering circuit 631 enciphers the data Dd inputted from the data input part 822 to data Dd# based on the key K which the key generation part 633 generatesand sends it out to the host computer 825.
[0173]The host computer 825 makes data Do# enciphered data Dd#and memorizes it to the memory 826. If enciphered data Do# which is memorized by the memory 826 is receivedthe decoding circuit 632 will be decrypted to the data Do based on the key K which the key generation part 633 generatesand will be told to the data output part 823. The data Do is the same as the data Dd. Thussince data is exchanged in the terminal unit 821 in the form enciphered between the host computers 825the barrier to disclosure of the information which data expresses is expensive.
[0174]The internal configuration of the key generation part 633 is shown by drawing 26. That isthe key generation part 633 generates the key K peculiar to a terminal unit using the electrical property which varies for every individual of the semiconductor device 401. Thereforeit is not necessary to write in the key Kand by the manufacturing process of the terminal unit 821since the semiconductor device 401 manufactured at the same process can be further used between the terminal units 821 of a large number mass-producedmanufacture of the terminal unit 821 can be simplified. Since the electrical property of the semiconductor device 401 which becomes a basis of the key K cannot be changed from the outsidethe advantage that the barrier to an unjust change of the key K is expensive is also acquired.
[0175]Drawing 32 is a block diagram showing another example of composition of the terminal unit by Embodiment 7. In the point that the key generation part 633 is included in IC card 829 which can be freely desorbed to the body part 828the terminal units of drawing 32 differ characteristic [the terminal unit 821 of drawing 31]. By equipping the body part 828 with IC card 829the enciphering circuit 631 and the decoding circuit 632 which were established in the body part 828 are connected to the key generation part 633.
[0176]Since the key generation part 633 is included in IC card 829 which can be freely desorbed to the body part 828it is possible by carrying IC card 829 convenient to carry free to use the same key K to two or more body parts 821 installed in the distant place.
[0177][8. embodiment 8] By Embodiment 8the memory 654 which memorizes the memory code Co explains the gestalt included in the auxiliary section which can be freely desorbed to a body part in the terminal unit 801 by Embodiment 4.
[0178]Drawing 33 is a block diagram showing the composition of the terminal unit by Embodiment 8. This terminal unit is equivalent to the device which is divided into the body part 651 and the battery charger 653 as an auxiliary sectionincluded semiconductor substrate CH50 in the body part 651 in the terminal unit 801 of drawing 20and included semiconductor substrate CH51 in the battery charger 653. The body part 651 is equipped with the cell which is not illustrated and which can be

chargedand the battery charger 653 charges a cellwhen the body part 651 is equipped.
[0179]When the body part 651 is equipped with the battery charger 653a cell is not only chargedbut between the semiconductor device 652 and semiconductor substrate CH51 which have semiconductor substrate CH50 is connected. The communication circuit 405a transmits only the identification signal Cd to the communication enterprise equipment 655 in the identification signal Cd and the memory code Cowhen the body part 651 is not equipped with the battery charger 653and when the body part 651 is equipped with the battery charger 653it transmits the both sides of the identification signal Cd and the memory code Co. The communication enterprise equipment 655the terminal unit body part 651and the battery charger 653 constitute the communications system 650.
[0180]Drawing 34 is a flow chart which shows the flow of processing until the terminal unit of drawing 33 is appropriated for the use to communication. Firstthe semiconductor device 652 as parts is manufactured (S501)the semiconductor device 652 is supplied to a telephone maker after thatand the terminal unit body part 651 is assembled by the telephone maker (S502). An average deed is carried out with thisit gets mixed upthe memory 654 as parts is manufactured (S503)and the battery charger 653 is assembled by the telephone maker after that (S504).
[0181]If the both sides of the terminal unit body part 651 and the battery charger 653 completethe identification signal Cd will be recorded on the memory 654 as the memory code Co (S505)and the set of the terminal unit body part 651 and the battery charger 653 will be supplied to the communication enterprise which holds the communication enterprise equipment 655 (S506). In one to Steps S501-S506 of stagesthe both sides of the identification signal Cd and the memory code Co are readand it is registered to the customer data memory 658 of the communication enterprise equipment 655 (S507). Thenafter the set of the terminal unit body part 651 and the battery charger 653 is supplied to a user (S508)it is appropriated for the use to communication by a user (S509).
[0182]Drawing 35 and drawing 36 are flow charts which show the internal procedure of Step S509. When communication is started and use of a terminal unit is use at the time of un-charging (i.e.when the body part 651 is not equipped with the battery charger 653)(S520) and the terminal unit body part 651 transmit the identification signal Cd to the communication enterprise equipment 655 (S521). In connection with itthe communication enterprise equipment 655 receives the identification signal Cd by the communication circuit 656 (S522).
[0183]Nextthe communication enterprise equipment 655 compares the identification signal Cd with the registered identification signal Cd by the decision circuit 657judges whether both sides are mutually in agreementand tells the decision signal En which shows a decision result to the communication circuit 656 (S523). When the decision signal En shows coincidence of numeralsthe user of (S524) and the terminal unit body part 651 performs attestation that he is a just userand the communication enterprise

equipment 655 does not perform (S524) and attestationwhen the decision signal En shows the disagreement of numerals. The communication enterprise equipment 655 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S525)and not attesting (S526).

[0184]When use of a terminal unit is use at the time of charge (i.e.when the body part 651 is used for communication in the state where it was connected to the battery charger 653)(S520S530)and the terminal unit body part 651 transmit the both sides of the identification signal Cd and the memory code Co to the communication enterprise equipment 655 (S531). In connection with itthe communication enterprise equipment 655 receives the identification signal Cd and the memory code Co by the communication circuit 656 (S532).

[0185]Nextthe communication enterprise equipment 655 judges whether by the decision circuit 657the identification signal Cd is compared with the registered identification signal Cdwhile judging whether both sides are mutually in agreementthe memory code Co is compared with the registered memory code Coand both sides are mutually in agreement. The decision circuit 657 tells the decision signal En expressing two decision results to the communication circuit 656 (S533).

[0186]Based on the decision signal Enwhen coincidence of numerals is accepted also in judgment [which]the communication enterprise equipment 655 (S534)The user of a terminal unit performs attestation that he is a just userand when the disagreement of numerals is accepted in one of judgments(S534) and attestation are not performed. Since a judgment is made in Step S533 based on the two numerals Cd and the both sides of Coonly based on the numerals Cdthe accuracy of a judgment is high compared with a judgment at Step S523. That isthe attestation made based on the judgment of Step S533 is equivalent to the high-ranking attestation (high level) which proves with higher accuracy that the terminal unit is used justly compared with the attestation made based on the judgment of Step S523.

[0187]Thereforethe communication enterprise equipment 655 becomes possible [using properly two attestation from which a level differs according to the importance of procedure]. As an examplewhen attesting based on the judgment of Step S533the communication enterprise equipment 655When the terminal unit is used for communicationpermit communication (S535) and it not only continues communications processing (S536)butIt is concerned with whether it is used for communicationand telex rate gold [as opposed to / there is nothing and / the communication before it (after being attested by last time based on the judgment of Step S533it communicates by this time)] is recorded as what was able to be supported (S537). It enables this to prevent the illegal act which escapes the obligation to pay a fee [loss of a terminal unit]. Since the case where the both sides of the terminal unit body part 651 and the battery charger 653 are lost simultaneously is rarebacking becomes a thing with accuracy high enough.

[0188]The communication enterprise equipment 655 records the identification signal Cd and the memory code Co which were received at Step S532 on the customer data memory 658 separately [the identification signal Cd and the memory code Co which have already been registered]when not attesting based on the judgment of Step S533. The identification signal Cd and the memory code Co which were recorded can be used for an unauthorized use person's specification.
[0189]It returns to drawing 34and in Step S507only the identification signal Cd may be registered instead of the both sides of the identification signal Cd and the memory code Co being registered. In this caseone to Steps S501-S506 of stages is sufficient if only the identification signal Cd is read. Registration of the memory code Co is attained by registering the memory code Co transmitted at Step S531 in the case of the use at the time of the first charge for a user to perform (S530) to the customer data memory 658.
[0190]The memory 601 may be included in a certain auxiliary section which can be freely desorbed not only to the battery charger 653 but to a body part. Howeverthe advantage that combination with the body part 651 and an auxiliary section is performed periodically is acquiredwithout an auxiliary section requiring time and effort special to a user in the gestalt of drawing 33 which is the battery charger 653.
[0191][9. embodiment 9] Embodiment 9 explains the gestalt from which numerals are transmitted in the enciphered form between a body part and an auxiliary section and between a body part and communication enterprise equipment in the terminal unit by Embodiment 8.
[0192]Drawing 37 is a block diagram showing the composition of the terminal unit by Embodiment 9. The enciphering circuit 631 and the key generation part 633 are formed in the semiconductor device 672 with which the body part 671 is providedand this terminal unit differs from the terminal unit of drawing 33 characteristic in the point that the enciphering circuit 631 and the key generation part 676 are formed also in the battery charger 653. In connection with itthe decoding circuit 632 is established in the communication enterprise equipment 675. The communication enterprise equipment 675the terminal unit body part 671and the battery charger 673 constitute the communications system 670.
[0193]In the battery charger 673the key generation part 676 generates the key K2 for encryptionand the enciphering circuit 631 enciphers the memory code Co read from the memory 601 based on the key K2and it sends it out to the body part 671 as memory code Co#. In the body part 671the key generation part 633 generates the key K1 for encryptionand the enciphering circuit 631 enciphers the identification signal Cd which the code generating part 400 generates based on the key K1and it tells it to the communication circuit 405a as identification signal Cd#. The enciphering circuit 631 of the body part 671 enciphers based on the key K1and also tells memory code Co# sent from the battery charger 673 to the communication circuit 405a as memory code Co##. Memory code Co## is doubly enciphered by the two keys K1 and K2.

[0194]The communication circuit 405a transmits identification signal Cd# and memory code Co## which were enciphered to the communication enterprise equipment 655. By the decoding circuit 632the communication enterprise equipment 655 decrypts identification signal Cd# and memory code Co## to the identification signal Cd and memory code Co#respectivelyand presents the material of a judgment in the decision circuit 657 with them.
[0195]Thusin the terminal unit of drawing 37since numerals are transmitted in the enciphered form between the body part 671 and the battery charger 673 and between the body part 671 and the communication enterprise equipment 675the advantage that the barrier to disclosure of these numerals is expensive is acquired.
[0196]In the body part 671the key generation part 633 and the enciphering circuit 631 are preferably formed in single semiconductor substrate CH50 (or CH70) with the code generating part 400. The key K1 and the barrier to disclosure of the identification signal Cd are further raised by it. Similarlyin the battery charger 673the key generation part 676 and the enciphering circuit 631 are formed in single semiconductor substrate CH71 with the memory 601. The key K2 and the barrier to disclosure of the memory code Co are further raised by it.
[0197]Drawing 38 is a flow chart which shows the flow of processing until the terminal unit of drawing 37 is appropriated for the use to communication. Firstthe semiconductor device 672 as parts is manufactured (S701)the semiconductor device 672 is supplied to a telephone maker after thatand the terminal unit body part 671 is assembled by the telephone maker (S702). An average deed is carried out with thisit gets mixed upthe memory 654 as parts is manufactured (S703)and the battery charger 673 is assembled by the telephone maker after that (S704).
[0198]If the both sides of the terminal unit body part 671 and the battery charger 673 completethe identification signal Cd will be recorded on the memory 654 as the memory code Co (S705)and the set of the terminal unit body part 671 and the battery charger 673 will be supplied to the communication enterprise which holds the communication enterprise equipment 675 (S706). In one to Steps S701-S706 of stagesthe identification signal Cdmemory code Co#and the key K1 are readand it is registered to the customer data memory 658 of the communication enterprise equipment 675 (S707). Thenafter the set of the terminal unit body part 671 and the battery charger 673 is supplied to a user (S708)it is appropriated for the use to communication by a user (S709).
[0199]Drawing 39 and drawing 40 are flow charts which show the internal procedure of Step S709. When communication is started and use of a terminal unit is use at the time of un-charging (i.e.when the body part 671 is not equipped with the battery charger 673)(S720) and the terminal unit body part 671 transmit identification signal Cd# to the communication enterprise equipment 675 (S721). In connection with itthe communication enterprise equipment 675 receives identification signal Cd# by the communication circuit 656 (S722).

[0200]Nextthe communication enterprise equipment 675 judges whether by the decision circuit 657the identification signal Cd is compared with the registered identification signal Cdand both sides are mutually in agreementafter decrypting identification signal Cd# to the identification signal Cd by the decoding circuit 632. And the decision circuit 657 tells the decision signal En which shows a decision result to the communication circuit 656 (S723). When the decision signal En shows coincidence of numeralsthe user of (S724) and the terminal unit body part 671 performs attestation that he is a just userand the communication enterprise equipment 675 does not perform (S724) and attestationwhen the decision signal En shows the disagreement of numerals. The communication enterprise equipment 675 stops communications processing by making communication into disapprovalwhen permitting communicationcontinuing communications processing for examplewhen attesting (S725)and not attesting (S726).

[0201]When use of a terminal unit is use at the time of charge (i.e.when the body part 671 is used for communication in the state where it was connected to the battery charger 673)(S720S730)The terminal unit body part 671 transmits the both sides of identification signal Cd# and memory code Co## to the communication enterprise equipment 675 (S731). In connection with itthe communication enterprise equipment 675 receives identification signal Cd# and memory code Co## by the communication circuit 656 (S732).

[0202]Nextby the decoding circuit 632the communication enterprise equipment 675 decrypts memory code Co## to memory code Co# while decrypting identification signal Cd# to the identification signal Cd. Thenthe communication enterprise equipment 675 judges whether by the decision circuit 657the identification signal Cd is compared with the registered identification signal Cdwhile judging whether both sides are mutually in agreementmemory code Co# is compared with registered memory code Co#and both sides are mutually in agreement. The decision circuit 657 tells the decision signal En expressing two decision results to the communication circuit 656 (S733).

[0203]Based on the decision signal Enwhen coincidence of numerals is accepted also in judgment [which]the communication enterprise equipment 675 (S734)The user of a terminal unit performs attestation that he is a just userand when the disagreement of numerals is accepted in one of judgments(S734) and attestation are not performed. The attestation made based on the judgment of Step S733 is equivalent to the high-ranking attestation (high level) which proves with higher accuracy that the terminal unit is used justly compared with the attestation made based on the judgment of Step S723.

[0204]As an examplewhen performing high-ranking attestation based on the judgment of Step S733the communication enterprise equipment 675When the terminal unit is used for communicationpermit communication (S735) and it not only continues communications processing (S736)butIt is concerned with whether it is used for

communicationand telex rate gold [as opposed to / there is nothing and / the communication before it (after being attested by last time based on the judgment of Step S733it communicates by this time)] is recorded as what was able to be supported (S737). When not performing high-ranking attestation based on the judgment of Step S733the communication enterprise equipment 675The identification signal Cd and the memory code Co which were received at Step S732 are recorded on the customer data memory 658 separately [the identification signal Cd and the memory code Co which have already been registered].

[0205]It returns to drawing 38and in Step S707only the identification signal Cd and the key K1 may be registered instead of the identification signal Cdmemory code Co#and the key K1 being registered. In this caseone to Steps S701-S706 of stages is sufficient if only the identification signal Cd is read. Registration of memory code Co# is attained by registering memory code Co# transmitted at Step S731 in the case of the use at the time of the first charge for a user to perform (S730) to the customer data memory 658.

[0206]As mentioned abovethe communication enterprise equipment 675 can use properly two steps of attestation from which accuracy differs like the case where the terminal unit of drawing 33 is usedby using the terminal unit of drawing 37 according to the importance of procedure. And since the identification signal Cd and the memory code Co are transmitted in the enciphered formthe barrier to disclosure of these numerals is expensive.

[0207]The case where it is required to exchange the battery charger 673 by losing the battery charger 673 or producing failure etc. is assumed. In such a caseif already registered memory code Co# can be updated to memory code Co# peculiar to the new battery charger 673it is convenient for a just user. As drawing 41 showsit is good for it to add Steps S741 and S742 to the procedure of drawing 40. in the procedure of drawing 41processing of Steps S731-S738 is performed like [when not changing memory code Co#] (S741) and drawing 41 -- change of memory code Co# -- **** -- unacquainted -- being alike -- processing which changes (S741) and registered memory code Co# is performed (S742).

[0208]Drawing 42 and drawing 43 are flow charts which show the internal procedure of change processing (S742). A start of change processing will transmit the requirement signal expressing the volition of change of memory code Co# registered with identification signal Cd#memory code Co##and a terminal identification number from a terminal unit to the communication enterprise equipment 675 (S752). In connection with itthe communication enterprise equipment 675 receives these numeralsa terminal identification numberand a signal by the communication circuit 656 (S753).

[0209]Nextby the decoding circuit 632the communication enterprise equipment 675 decrypts memory code Co## to memory code Co# while decrypting identification signal Cd# to the identification signal Cd. Thenthe communication enterprise

equipment 675 judges whether by the decision circuit 657the identification signal Cd is compared with the registered identification signal Cdwhile judging whether both sides are mutually in agreementmemory code Co# is compared with registered memory code Co#and both sides are mutually in agreement. The decision circuit 657 tells the decision signal En expressing two decision results to the communication circuit 656 (S753).

[0210]When coincidence of numerals is accepted also in judgment [which] based on the decision signal Enwhile the communication enterprise equipment 675 transmits the notice of a purport which permits change of (S754) and registered memory code Co# to a terminal unitThe message which stimulates the exchange to the battery charger 673 with new memory code Co# is transmitted and displayed on a terminal unit. According to itthe battery charger 673 with which the user of a terminal unit has memory code Co#If it exchanges to the battery charger 673 which has new memory code Co# (it is indicated as CoNew# for convenience) (S757)identification signal Cd# and memory code CoNew## will be transmitted to the communication enterprise equipment 675 from a terminal unit (S758). In connection with itthe communication enterprise equipment 675 receives these identification signal Cd# and memory code CoNew## by the communication circuit 656 (S753).

[0211]Nextby the decoding circuit 632the communication enterprise equipment 675 decrypts memory code CoNew## to memory code CoMew# while decrypting identification signal Cd# to the identification signal Cd (S760). Thenthe communication enterprise equipment 675 updates memory code Co# registered to the customer data memory 658 by memory code CoNew#.

[0212]Based on the decision signal Enwhen the disagreement of numerals is accepted in one of judgmentsthe communication enterprise equipment 675 (S754)The message urged that operation for the second time is performed using the battery charger 673 present in use as it is is transmitted and displayed on a terminal unitwithout advancing change processing more (S755).

[0213]The same change processing as Step S742 can be added not only to the procedure of drawing 40 but to the procedure of drawing 36 which does not use a code. Therebya user becomes possible [exchanging the battery charger 653 of drawing 33].

[0214]Instead of using OTPROM for the memory 654 with which the battery charger 653673 is provideda rewritable memoryfor examplea flash ROMmay be used. The above-mentioned change processing S742 is suitable also for use of the battery charger 653673 which can rewrite such memory code Co#. In order to raise the security to an unjust changeit is also possible to limitwhen a terminal unit transmits the information which can guarantee fee collectionsuch as a credit card numberfor rewriting of registered memory code Co#.

[0215]Drawing 44 and drawing 45 are flow charts which show another internal flow of the communications processing (S709) of drawing 38. Attestation is used for a

commercial transaction in this communications processing (S770). When performing high-ranking attestation based on the judgment of Step S733the communication enterprise equipment 675 Namely(S734)continuing (S735) and communications processingwhen the terminal unit is used for communication -- a commercial transaction -- granting a permission (S736). It is concerned with whether the terminal unit is used for communicationand records as that in which the commercial transaction made [in / there is nothing and / the communication before it (after being attested by last time based on the judgment of Step S733it communicates by this time)] was materialized (S775). On the other handthe communication enterprise equipment 675 is recorded as that in which the commercial transaction made in communication before it was not materializedwhen not performing high-ranking attestation based on the judgment of Step S733 (S776).

[0216]If record of the purport that the commercial transaction was materialized based on highly accurate attestation is madeIf business contacts have record of the purport that the commercial transaction can advance various proceduresuch as dispatch of goodsas an effective thingand a commercial transaction was not materializedbased on the record concernedthey can stop the procedure based on a commercial transaction. Therebythe damage caused by the unjust commercial transaction based on the unauthorized use of a terminal unit can be canceled thru/or reduced.

[0217]Still more desirablythe communication enterprise equipment 675 performs record for also making improper the commercial transaction at the time of un-chargingwhen not performing high-ranking attestation based on the judgment of Step S733 (S777). Record is performed byfor examplesetting a flag to the register of the computer system with which the communication enterprise equipment 675 is provided.

[0218]When use of a terminal unit is use at the time of un-charging (i.e.when the body part 671 is not equipped with the battery charger 673)(S720)When attesting based on the judgment of Step S723it is judged whether the record which makes improper the commercial transaction at the time of un-charging is made (S771). (for exampledoes the above-mentioned flag stand or not?) And the communication enterprise equipment 675 will stop communications processingif the above-mentioned record is not madecommunications processing is continueda commercial transaction is permitted (S772) and record is made (S773).

[0219]Thussince a decision result with high accuracy made in the past is reflected in the usual attestation made in the state where the body part 671 is not equipped with the battery charger 673important proceduresuch as a commercial transactioncan be performed under the usual attestation. Also in Step S509 shown in drawing 35 and drawing 36it is possible to perform Steps S772-S773S774 - S777 which were shown in drawing 44 and drawing 45.

[0220]The battery charger 673 of drawing 37 can also be transposed to an IC card convenient to carry. In this casealthough a user needs to equip the body part 671 with an IC card occasionallyIf it is possible to perform transmission of memory code

Co# from an IC card to the body part 671 through radioa user can save the time and effort which equips the body part 671 with an IC card intentionallyand is convenient for a user. Drawing 46 is a block diagram which illustrates the terminal unit constituted such.

[0221]The communication interface 694 is formed in the semiconductor device 692 with which the body part 691 is provided with the terminal unit of drawing 46and the communication interface 695 is formed also in IC card 693. The communication interface 694 is formed in single semiconductor substrate CH90 (or CH91) with the key generation part 633the enciphering circuit 631and the code generating part 400for example. Similarlythe communication interface 695 is formed in single semiconductor substrate CH92 with the key generation part 676the enciphering circuit 631and the memory 601for example.

[0222]The communication interface 694695 is an interface which performs radiofor exampleis based on the Bluetooth standard. Thereforetransmission of memory code Co# from IC card 693 to the body part 691 is performed by carrying radio. For this reasonfor exampleIC card 693 is supplied in the pocket of a user's clothesand even if the body part 691 is stored in the bag which a user carriesit becomes possible to transmit the both sides of identification signal Cd# and memory code Co## to the communication enterprise equipment 675. A card like UIM (Universal subscriber Identification Module) used inserting in the body part as a portable telephone instead of IC card 693 may be used. Howeversince a possibility that a user will lose a body part and a card simultaneously cannot be disregarded in that caseas drawing 46 showsthe gestalt which exchanges memory code Co# between separate independent apparatus is more desirable.

[0223]In the communications system 670as drawing 12 showsthe communication enterprise equipment 655 can be replaced to other entrepreneur equipmentsuch as an ATM system of a bank. For examplewhen performing a commercial transaction based on attestationthe ATM system of the bank which is business contacts of a terminal unit is able to perform directly processing of attestation and permission of a commercial transactiondisapprovaletc. Also in the communications system in other embodimentsit is the same.

[0224][10. embodiment 10] In the formerthe terminal unit had the problem that radio which carried communication enterprise equipment could not be performedin fields upon which an electric wave cannot trespass easilysuch as inside of an underground center or a building. Or in order to make radio possible in such a fieldmany base stations needed to be provided. Also in the field which cannot perform radio which carried communication enterprise equipmentEmbodiment 10 explains the terminal unit and correspondence procedure which make radio possible without a base station. In the terminal unit and correspondence procedure by this embodimentthe enciphering circuitdeccding circuitand key generation part which were shown by Embodiment 5 etc. play a useful role.

[0225][10.1. outline] Drawing 47 is an explanatory view showing the correspondence procedure by this embodiment. In this methodthe terminal unit which can form the radio which carried communication enterprise equipmentand the wireless communication network which does not carry communication enterprise equipment is used. In the example explained belowwireless LAN is adopted as the above-mentioned wireless communication network. Sometimes also in the field upon which an electric wave cannot trespass easilythe crowd is usually gathering thru/or passing. in the presentthese crowds' ****** in few are carrying the portable telephone. If the portable telephone which these crowds carry is a terminal unit which has the above-mentioned functionas drawing 47 showsit will become possible by forming wireless LAN among two or more terminal units 840a-840d to communicate mutually. For examplethe terminal unit 840a and the terminal unit 840d become possible [communicating mutually] by relaying the terminal units 840b and 840c.
[0226]As wireless LANwhat was basedfor example on the Bluetooth standard can be used. In this caseone terminal unit can be communicated with other terminal units which exist within a 10-m radius centering on self by carrying radio. In an underground center or a buildingsometimesmany passing personsa workeretc. usually exist within 10 mand the communication which covers the whole inside of an underground center or a building is attained by going via the terminal unit which these people carry.
[0227]By using wireless LANthe advantage that it is manageable with small electric power is also acquired. For examplein the wireless LAN which makes 10 m a range of accessthe power consumption taken to discharge an electric wave is $^{(1/100)2}$ twice compared with the radio which makes 1 km a range of access. In order to communicate between the 1-km-away terminal unitseven if 1000 terminal units located in a line at intervals of an average of 1 m relay communicationtotal power consumption is reduced by $^{(1/100)\ 2}$x1000=1 / 10 times.
[0228]Communication which carried terminal units in the above-mentioned whole space is realized by forming wireless LAN not only in the field upon which an electric wave like [in an underground center or a building] cannot trespass easily but in the space in which many people generally gatherpass thru/or reside. Even if there is a field where an electric wave like [in an underground center or a building] cannot invade easily into the space concernedthe communication which carried terminal units is not checked. When a terminal unit domestic [each] relays wireless LANalso in a terrestrial residential streetthe radio communications system of the low power consumption which a base station hardly needs can be built.
[0229][Example of a 10.2. terminal unit In the communication which carried the wireless LAN which drawing 47 showssince communication is performed via the terminal unit which many and unspecified persons carryit is necessary to secure the security to disclosure of a communication content.] As drawing 48 showsit is good for it for the portion (the long distance communications department is called tentatively)

847 which performs radio which carried communication enterprise equipmentand the portion (a short distance communication part is called tentatively) 848 which performs communication which carried wireless LAN to constitute the terminal unit 480 so that it may dissociate electrically.
[0230]The input part 845 for inputting the loudspeaker 843 for outputting the microphone 842 for the long distance communications department 847 to input the communication circuit 841 and sound which perform radio which carried communication enterprise equipmentand a sounda number to be dialedetc. by key operation etc. and a charactera signIt has the display panel 844 which displays information with a figure etc. The short distance communication part 848 is provided with the wireless LAN circuit 846 which performs radio by forming wireless LAN. In the terminal unit 840 of drawing 48since it dissociates mutuallythe user itself who possesses the terminal unit 840 cannot perform communication which carried wireless LANbut the long distance communications department 847 and the short distance communication part 848 only bear the role which only relays others' communication.
[0231]In order for the possessor of a terminal unit itself to make it possible to perform communication which carried wireless LAN and to secure the security to disclosure of a communication content moreoveras drawing 49 showsit is good to use encoding technology. Even if it is a case where encoding technology is used by the radio through communication enterprise equipmentdifferent original cipher systems from it are used for communication through wireless LAN.
[0232]The channels of communication of signal transmission are established between the wireless LAN circuit 846 and the communication circuit 841and the switching circuit 856the enciphering circuit 851and the decoding circuit 852 are inserted in these channels of communication. The switching circuit 856 performs connection and cutting of the above-mentioned channels of communicationenabling free selection. When the switching circuit 856 connects the above-mentioned channels of communicationcommunication which carried wireless LAN is realized between the user of the terminal unit 850and the others. When the switching circuit 856 cuts the above-mentioned channels of communicationthe terminal unit 850 only relays communication of the others which carried wireless LAN. In drawing 49for convenience although an antenna is divided and drawn on the object for transmissionand receptionthese are communalized by the single antenna in usual.
[0233]In order to perform communication which carried wireless LAN between the user of the terminal unit 850and the othersthe enciphering circuit 851the decoding circuit 852and the key generation part 853 achieve the functionwhen the switching circuit 856 connects the above-mentioned channels of communication. The key generation part 853 generates the key K for encryption. The enciphering circuit 851 enciphers the sending signal sent to the sending circuit 855 of the wireless LAN circuit 846 based on the key K from the communication circuit 841. The decoding circuit 852 decrypts the input signal sent to the communication circuit 841 based on

the key K from the receiving circuit 854 of the wireless LAN circuit 846.
[0234]Herethe keys K need to be a communications partner which carries wireless LAN and with which the terminal unit 850 communicatesand a common key. Therefore the key generation part 853 has an internal configuration which drawing 50 shows. That isthe key generation part 853 is provided with the code generating part 633 and the key operation part 857. The code generating part 633 generates the identification signal Cd peculiar to the terminal unit 850. Based on another numerals sent from a communications partner through the wireless LAN circuit 846between the user of the terminal unit 850and a communications partnerthe key operation part 857 computes a common key usable in commonand outputs it as the key K.
[0235]As for the code generating part 633it is desirable to take the gestalt shown in drawing 25 or drawing 26 of Embodiment 5. Therebythe same effect as Embodiment 5 is acquired. Drawing 50 shows the example in which the code generating part 633 was formed on a par with drawing 26.
[0236][Procedure of 10.3. key generation] Drawing 51 is a flow chart which shows an example of the procedure in which the key generation part 853 generates the key K. The procedure of drawing 51 uses the well-known DH process. If the communication which carried wireless LAN is started between the terminal unit 850 and other terminal unitsit will be judged whether it is newother terminal unitsi.e.communications partner(S801). If the communications partner is newnumerals alpha#=galphamod (p) will be computed by the key operation part 857 based on the natural number g beforehand determined as the prime number p defined beforehand (S802). Herealpha is the identification signal Cd which the code generating part 633 generates. mod() expresses the mode in a theory of numbers. The prime number p and the natural number g are common among all the terminal unitsand equivalent to a public key.
[0237]Nextcomputed numerals alpha# is transmitted to a communications partner through the communication circuit 841 and the sending circuit 855 (S803). It continuesand it is received by the receiving circuit 854 and numerals beta#=gbetamod (p) which the communications partner transmitted is sent to the key operation part 857 through the communication circuit 841 (S804). Nextthe key operation part 857 computes key K=g****mod (p) (S805). Thenthe key operation part 857 records the computed key K on the memory 858 with the identification number (for exampletelephone number) of a communications partner (S806).
[0238]Nextthe key operation part 857 realizes encryption communication which uses the key K as a common key by supplying the key K to the enciphering circuit 851 and the decoding circuit 852 (S808). Processing of Step S808 is continued until communication is completed (S809). In Step S801if judged with a communications partner not being newwithout computing the key Kthe key operation part 857 will read the key K currently recorded on the memory 858 (S807)and will perform processing of Step S808 and S809. The judgment of Step S801 can be performed based on whether record exists in the memory 858.

[0239]As mentioned abovecommunication with arbitrary communications partners is realizablepreventing disclosure of a communication contentsince encryption communication is performed based on the common key generated by exchanging a communications partner and an identification signal. Whenever it removes Steps S801 and S807 in a procedure to drawing 51 and communication is performedit is also possible tc compute the key K.
[0240][Another example of a 10.4. terminal unit] Drawing 52 is a block diagram showing another example of composition of the terminal unit of Embodiment 10. In this terminal unit 860the input signal which the communication circuit 861 receivedIt is amplified with the low noise amplifier (Low Noise Amplifier) 862and after getting over by the mixer 863 combined with VCO(Voltage Controlled Oscillator; voltage-controlled oscillator) 864it is processed in the baseband circuit 878. It becomes irregular by the mixer 865 combined with VCO866and after the sending signal processed in the baseband circuit 878 is amplified with the power amplifier (Power Amplifier) 867it is transmitted to communication enterprise equipment.
[0241]On the other handthe input signal which the wireless LAN circuit 871 received is amplified with the low noise amplifier 872and after getting over by the mixer 873 combined with VCO874it is modulated by the mixer 868 combined with VCO869 via the switching circuit 870. The modulated input signal is inputted into the baseband circuit 878 through the mixer 863 of the communication circuit 861. The input signal of wireless LAN inputted into the baseband circuit 878 is decrypted by the decoding circuit 852 The sending signal of wireless LAN is inputted into the baseband circuit 879 through the enciphering circuit 851 and the switching circuit 856 from the baseband circuit 878. Thenit becomes irregular by the mixer 875 combined with VCO766and this sending signal is transmitted after being amplified with the power amplifier 877.
[0242]As mentioned aboveit becomes irregular and the terminal unit 860 of drawing 52 is inputted into the communication circuit 861after the input signal inputted into the wireless LAN circuit gets over. As drawing 53 showsthe mixer 858 is modulated using the subcarrier which has the frequency f in the specific range (it describes "it is a band specially" at drawing 53) set up in the zone for communication circuits in the input signal of the wireless LAN to which it restored. For this reasoneven if the frequency f of the input signal of wireless LAN is in which range within the zone for wireless LAN circuitsthe modulated wave which has the frequency f within the limits of a band specially is inputted into the communication circuit 861.
[0243]When only conversion of frequency is performed and it inputs into the communication circuit 861 temporarilywithout restoring to the input signal of wireless LANas drawing 54 showsit is necessary to secure the band for communication circuits widely. On the other handit is not necessary to secure the band for communication circuits widelyand the advantage that the utilization ratio of the frequency band of the communication circuit 861 can be raised is acquired in the

terminal unit 860 of drawing 52.
[0244]As drawing 55 showswith the terminal unit which the communication circuit and the wireless LAN circuit combined enabling free selectionit also becomes possible to combine the communication path and wireless LAN through communication enterprise equipmentso that it may be illustrated by drawing 49 or drawing 52. That iscommunication through communication enterprise equipment of another terminal unit 850a can be performed through the communication circuit of the long distance communications department 847 of the terminal unit 850c which are some of two or more terminal units 850a-850c which form wireless LAN. Thusthe terminal unit in the underground center etc. upon which an electric wave cannot trespass easily is possible also for performing communication which carried communication enterprise equipment. In order to make light the burden of the terminal unit (the example of drawing 55 terminal unit 850c) which combines the communication path and wireless LAN through communication enterprise equipmentsuch communication may be permitted only within urgent emergency traffic.
[0245]It is also possible to restrict all communications that lead wireless LAN to urgent emergency traffic. The burden of the terminal unit (the example of drawing 47 terminal units 840b and 840c) which relays communication through wireless LAN by it is mitigable. In urgent emergency trafficsince the importance of the security to disclosure of a communication content is lowit also becomes possible to remove the circuit for encryption. Urgent emergency traffic is communication aiming at the request etc. of the rescue accompanying generating of the state of emergency which threatens a life and propertyfor example.
[0246][11. embodiment 11] Also in fields to which it is assumed that many crowds usually sometimes concentratesuch as inside of an underground center and a buildinga crowd's density is reducedfor example depending on time zonessuch as night. By Embodiment 11in the field upon which an electric wave cannot trespass easilyalso when a crowd's density is lowthe correspondence procedure which enables communication through wireless LAN is explained.
[0247]Drawing 56 is an explanatory view showing the correspondence procedure by an embodiment. In this correspondence procedurethe terminal units 1050a and 1050b which enable formation of wireless LAN are installed in the field upon which the electric wave of an underground center etc. cannot trespass easily. Preferablythe terminal units 1050a and 1050b are public telephonesfor exampleare installed near the entrance of the store of an underground center. In this casethe terminal units 1050a and 1050b are provided with the long distance communications department 1057 which attains the original function of a public telephone with the short distance communication part 848. Even when a crowd's density is lowthe terminal unit 850a and the terminal unit 850b can perform communication which carried wireless LAN by relaying the short distance communication part 848 of the terminal units 1050a and 1050b.

[0248][12. embodiment 12] Embodiment 12 explains a still more desirable gestalt about the semiconductor device 401 explained by an above embodimentthe coding circuit 402and the comparison circuit 403.
[0249][Example of a 12.1. semiconductor device] Drawing 57 is a circuit diagram showing a desirable example of the semiconductor device 401. This semiconductor device 401a is provided with two or more TFT(example of drawing 57 4x4 pieces = 16 pieces)101 arranged by matrix form on the substrate. On the substratefurther two or more word lines WL1-WL4 and two or more bit lines BL1-BL4 are arranged by the transverse direction and the lengthwise directionrespectively.
[0250]Four gate electrodes of TFT101 arranged to a ****** single tier are connected to each of the word lines WL1-WL4 in common. On the other handfour drain electrodes of TFT101 arranged to a ****** single tier are connected to each of the bit lines BL1-BL4 in common. 16 source electrodes of TFT101 are connected to the positive supply line in common. Each end of the bit lines BL1-BL4 is connected to the grounding power supply line through the bit line load 7.
[0251]The wiring 18 for taking out the analog signal An is connected with the earthing conductor of the bit line load 7 at the end of the opposite hand. The pad 15 is connected to each other end of the bit lines BL1-BL4and the pad 16 is connected to each one end of the word lines WL1-WL4.
[0252]Since the semiconductor device 401a is constituted as mentioned abovethe drain current Id1-Id4 flows through it into four TFT101 connected to the word linerespectively by giving the gate voltage of predetermined height to one in the word lines WL1-WL4. Since the drain current Id1-Id4 flows through the bit line load 17in the wiring 18 connected to the bit lines BL1-BL4the potential proportional to the drain current Id1-Id4 generates itrespectively. This potential of four pieces is outputted to the exterior as the analog signal An. The potential of a total of 16 pieces can be taken out as the analog signal An by giving gate voltage to the word lines WL1-WL4 one by one.
[0253]When coded by the coding circuit 402the 16 analog signals An are changed into a 16-bit digital signalfor example so that drawing 58 may illustrate. 16-bit numerals are arranged to matrix formand drawing 58 is shown so that the relation between TFT101 which becomes a basis of numeralsand the bit lines BL1-BL4 and the word lines WL1-WL4 which are connected to it may be known.
[0254][Example of a 12.2. coding circuit and a comparison circuit] Drawing 59 is a block diagram showing the desirable gestalt of the semiconductor device which uses as a semiconductor substrate semiconductor substrate CH3 (or CH1) shown in drawing 1. This semiconductor device 404a is provided with the semiconductor device 401a shown in drawing 57. The semiconductor device 404a is equipped with the decoder driver 410 which drives arbitrary one of two or more of the word lines WL1-WL4 with which the semiconductor device 401a is equipped based on the address signal Adr. The address signal Adr can be inputted from the outside through an input

terminal.
[0255]The numerals Cd which the coding circuit 402 outputs are not only inputted into the comparison circuit 403but are outputted to the exterior via the buffer circuit 411. Therebythe person of the limited range becomes possible [getting to know the identification signal Cd beforehand]. Since the buffer circuit 411 is equippedthe malfeasance of inputting into the comparison circuit 403 from the exterior numerals which are different in the identification signal Cd which the coding circuit 402 outputs through the output terminal of the identification signal Cd can be prevented.
[0256]Since the semiconductor device 401a is equipped with the pads 15 and 16in the process in which the semiconductor device 404a is manufacturedit is also possible by applying a probe to these pads 15 and 16 to read the analog signal An directly. The read analog signal An can be changed into the identification signal Cd using a device with the same characteristic as the coding circuit 402and it is also possible for this to acquire the identification signal Cd. Thereforeas long as read-out of the identification signal Cd does not need to be performed except the plant of the semiconductor device 404athe input terminal of the address signal Adrthe output terminal of the identification signal Cdand the buffer circuit 411 may be removed.
[0257]When the comparison circuit 403 compares with the identification signal Cd the memory code Co inputted through an input terminalit inputs the address signal Adr into the decoder driver 410. Since the semiconductor device 404a drives and the analog signal An is read by that causeeven if it does not input the address signal Adr from the exteriorit becomes possible to perform comparison between the identification signal Cd and the memory code Co.
[0258]Drawing 60 is a circuit diagram showing the desirable gestalt of the coding circuit 402and is drawing the portion connected to bit line BL1 as a representative. The same circuit part as drawing 60 is connected to other bit lines BL2-BL4. This coding circuit 402a is equipped with the sense amplifier 190. The sense amplifier 190 compares the potential of the wiring 18 with the reference potential Vref which the transistor 192193 generatesgenerates the signal of high level or a low leveland outputs it as 1 bit (for exampleidentification signal Cd corresponding to bit line BL1 (1)) of the identification signal Cd.
[0259]In the sense amplifier 190the series circuit of NMOS transistor 194 and PMOS transistor 195 and the series circuit of NMOS transistor 196 and PMOS transistor 197 are inserted between the grounding power supply line and the positive supply line. And the current mirror circuit is formed by connecting mutually the gate electrode of PMOS transistor 195a drain electrodeand the gate electrode of PMOS transistor 197.
[0260]The drain current which flows through TFT101 is a low value of about 1 pA (10^{-2}A) - about 1microA within the limits. Thereforeit is desirable by impressing constant potential to the gate electrodeusing an NMOS transistor as the bit line load 17 to set the drain current as about 1 nA (10^{-9}A) grade. The sensitivity of the sense amplifier 190 is raised by it. As for gate potentialwhen setting drain current as about 1 nAit is

desirable to consider it as earth potentials.
[0261]The series circuit of NMOS transistor 192 and PMOS transistor 193 is inserted between the grounding power supply line and the positive supply lineand the reference potential Vref is taken out from the terminal area of these two transistors. Constant potentialsuch as potential of a grounding power supply line and potential of a positive supply lineis supplied to the gate electrode of NMOS transistor 192 and PMOS transistor 193respectively. It is equivalent to the reference current Ir (or the fixed multiple) which flows through the series circuit of the drain currentNMOS transistor 192and PMOS transistor 193 of TFT101 being compared that the potential of the wiring 18 is compared with the standard ionization Vref.
[0262]As for transistors other than TFT101 drawn on drawing 60when performing stable comparisonit is desirable to be constituted as a bulk type transistor which is not a TFT type. If transistors other than TFT101 are formed as the polycrystal TFT as well as TFT101in order to make the size of those drain current stableAs for those gate length and gate widthit is desirable to be set up more greatly than the gate length and gate width of TFT101.
[0263][Another example of a 12.3. semiconductor device] The semiconductor device 401 may be provided with the resistance element of the polycrystalline substanceor the capacitor (capacitative element) of the polycrystalline substancefor example instead of having polycrystallized type TFT101. Belowsuch an example is explained.
[0264]Drawing 61 is a circuit diagram in which the semiconductor device 401 shows an example provided with the resistance element of the polycrystalline substance. In this semiconductor device 401bit has on the substrate two or more resistance elements (the example of drawing 61 4x4 pieces = 16 pieces) 43 arranged by matrix form. In the resistance element 43the resistor is formed with the polycrystalline semiconductorfor examplepolycrystalline silicon. For this reasonresistance differs in the resistance element 43 at random.
[0265]On the substratefurther two or more word lines WL1-WL4 and two or more bit lines BL1-BL4 are arranged by the transverse direction and the lengthwise directionrespectively.
[0266]The end of the four resistance elements 43 arranged to a ****** single tier is connected to each of the word lines WL1-WL4 in common. On the other handthe other end of the four resistance elements 43 arranged to a ****** single tier is connected to each of the bit lines BL1-BL4 in common. Each end of the bit lines BL1-BL4 is connected to the grounding power supply line through NMOS transistor 48 as bit line load. The gate electrode of NMOS transistor 48 is connected to a grounding power supply linefor example.
[0267]The wiring 49 for taking out the analog signal An is connected to the drain electrode of NMOS transistor 48. The pad 15 is connected to each other end of the bit lines BL1-BL4and the pad 16 is connected to each one end of the word lines WL1-WL4.

[0268]Since the semiconductor device 401b is constituted as mentioned abovecurrent flows through it into the four resistance elements 43 connected to the word line by giving the gate voltage of predetermined height to one in the word lines WL1-WL4. Since these current flows through NMOS transistor 48to each of the wiring 49 connected to the bit lines BL1-BL4the potential proportional to the current which flows through the resistance element 43 generates it. This potential of four pieces is outputted to the exterior as the analog signal An. The potential of a total of 16 pieces can be taken out as the analog signal An by giving predetermined potential to the word lines WL1-WL4 one by one. The analog signal An is acquired as a random value corresponding to dispersion in resistance of the resistance element 43.
[0269]Since the pads 15 and 16 are equippedit is also possible to read the analog signal An in the manufacturing process of the semiconductor device 401b using a probe. The resistance element 43 may be arranged by one-dimensional matrix formand may be connected to a word line with a single end of all the resistance elements 43. In order to enlarge dispersion in the analog signal Anit is good to set the length and width of the polycrystalline substance which the resistance element 43 has as the same range as the optimal condition over gate length L and gate width W.
[0270][Another example of a 12.4. semiconductor device] Drawing 62 is a circuit diagram in which the semiconductor device 401 shows an example provided with the capacitative element of the polycrystalline substance. In this semiconductor device 401cit has on the substrate two or more capacitative elements (the example of drawing 61 4x4 pieces = 16 pieces) 91 and the series circuit of MOS transistor 90 which were arranged by matrix form. The capacitative element 91 is equipped with perovskite-type polycrystal dielectricssuch as a polycrystal dielectric ($Ba_xSr_{1-x}TiO_3$)for exampleBST etc. For this reasoncapacity value differs in the capacitative element 91 at random.
[0271]On the substratefurther two or more word lines WL1-WL4 and two or more bit lines BL1-BL4 are arranged by the transverse direction and the lengthwise directionrespectively. The gate electrode of MOS transistor 90 belonging to four series circuits arranged to a ****** single tier is connected to each of the word lines WL1-WL4 in common. On the other handthe source electrode of MOS transistor 90 and the one side electrode of a drain electrode belonging to four series circuits arranged to a ****** single tier are connected to each of the bit lines BL1-BL4 in common. The end of the capacitative element 91 belonging to 16 series circuits is connected to the grounding power supply line. The pad 15 is connected to each other end of the bit lines BL1-BL4and the pad 16 is connected to each one end of the word lines WL1-WL4.
[0272]Since the semiconductor device 401c is constituted as mentioned aboveit can make four MOS transistors connected to the word line the one by giving the gate voltage of predetermined height to one in the word lines WL1-WL4. The other end of the four capacitative elements 91 is electrically connected to the bit lines BL1-BL4

through the MOS transistor [one / the MOS transistor]. At this timethe capacity (capacitance) of the four capacitative elements 91 is measurable through the bit lines BL1-BL4. For exampleit is good to be able to measure potential when current is supplied over fixed timeand to take out this potential as the analog signal An. The capacity of the capacitative element 91 is reflected in this potential.

[0273]The potential of a total of 16 pieces can be taken out as the analog signal An by giving predetermined gate voltage to the word lines WL1-WL4 one by one. The analog signal An is acquired as a random value corresponding to dispersion in the capacity of the capacitative element 91. Since the pads 15 and 16 are equippedit is also possible to read the analog signal An in the manufacturing process of the semiconductor device 401c using a probe. The series circuit of the capacitative element 91 and MOS transistor 90 may be arranged by one-dimensional matrix formand the gate electrode of all the MOS transistors 90 may be connected to a single word line.

[0274]In order to enlarge dispersion in the analog signal Anit is good to set the length and width of a polycrystal dielectric which the capacitative element 91 has as the same range as the optimal condition over gate length L and gate width W. In BSTwhen the thickness is 100 nmthe thickness converted into silicon oxide is about 0.5 nm. Thereforethe capacity will be set to about 6.2 fF supposing the shape of BST which faces an electrode is a square whose one side is 0.3 micrometer. The capacity differs in the optimal case where a crystal grain diameter (average value) is set as 100 nm equivalent to thicknessin the range of -30%-+30% of the rangei.e.4.3fF- 8.1fF. It can be said that this value is dispersion in sufficient size to use as discernment.

[0275][Another example of a 12.5. comparison circuit] Drawing 63 is a block diagram showing another desirable gestalt of the semiconductor device which uses as a semiconductor substrate semiconductor substrate CH3 (or CH1) shown in drawing 1. The comparison circuit 403a with which this semiconductor device 404d is provided is constituted so that not only the full match nature of the identification signal Cd and the memory code Co but the approximation nature in the range defined beforehand can be judged. Reference-value SL of a judgment can be inputted from the outside of the semiconductor device 404d through an input terminal.

[0276]In order to make this possiblethe comparison circuit 403a is provided with the sweep circuit 200 which carries out the sweep of the potential of the word line WL. The identification signal Cd which changes by carrying out the sweep of the potential of the word line WL is compared with the part where the memory code Co held at the input code memory 198 corresponds by the order-of-approximation calculation circuit 199. The order-of-approximation calculation circuit 199 transmits order-of-approximation VA between both numerals computed through comparison to the weighting network 210. By comparing order-of-approximation VA with reference-value SLthe weighting network 210 judges whether order-of-approximation VA is more than fixedand outputs the result as decision signal VB.

[0277]Decision signal VB is individually obtained for every word line WL which the decoder driver 410 drives. The address generation circuit 441 transmits the address signal which specifies every one word lines WL of all the in order to the decoder driver 410. Therebytwo or more one decision signal VB of every corresponding to all the word lines WL is obtained in order.
[0278]Based on two or more decision signal VB corresponding to all the word lines WLthe comprehensive decision circuit 220 judges the approximation nature between the numerals Cd of all the bits corresponding to all the word lines WLand the numerals Co of all the bitsand outputs the decision signal En expressing the result. By setting up reference-value SL appropriatelyit is also possible to choose the judgment of the severest full match nature as a judgment of approximation nature. If the word line is singlethe comprehensive decision circuit 220 will be unnecessary and decision signal VB will be outputted as the decision signal En as it is.
[0279]The control circuit 442 controls operation of each element to meet a predetermined procedure while it answers indication signal St inputted through an input terminal and makes operation of each element of the comparison circuit 403a start. Sweep switch signal SS which directs whether perform a sweep from the control circuit 442 to the sweep circuit 200 especially and which is a control signal is transmitted. The order-of-approximation calculation circuit 199the weighting network 210and the comprehensive decision circuit 220 constitute the decision circuit 440.
[0280]
[Effect of the Invention]In the device of the 1st inventionsince the numerals for identifying a semiconductor substrate are memorized by another semiconductor substratethe malfeasance of using the applied machine with which this device was incorporated for a semiconductor substrate exchanging can be prevented by comparing these numerals.
[0281]Since a memory memorizes numerals to OTPROM in the device of the 2nd inventionthe barrier to an unjust change of the numerals memorized by the memory is expensive.
[0282]In the device of the 3rd inventionsince an identification signal is generated using dispersion in the electrical property of a semiconductor devicethe semiconductor device manufactured at the same process can be used between these devices of a large number mass-produced. For this reasonmanufacture of a device is simplified. Since the electrical property of the semiconductor device which becomes a basis of an identification signal cannot be changed from the outsidethe barrier to an unjust change of an identification signal is expensive.
[0283]Since a semiconductor device has the polycrystalline substance and an identification signal is generated in the device of the 4th invention using dispersion in the crystal structuredispersion in the electrical property between the semiconductor devices manufactured at the same process is large. For this reasonit is easy to keep an identification signal from being mutually in agreement between these devices of a

large number mass-produced.
[0284]Since a code generating part memorizes an identification signal to OTPROM in the device of the 5th inventionthe barrier to an unjust change of the identification signal which a code generating part generates is expensive.
[0285]In the device of the 6th inventionsince the judgment of the conformity of numerals is performed by the comparison circuita decision signal can be used for attestation by it.
[0286]In the device of the 7th inventionsince the comparison circuit is formed in the semiconductor substrate in which the code generating part is formedthe identification signal inputted into a comparison circuit from a code generating part in the same semiconductor substrate cannot be unjustly changed from the outside. For this reasonthe barrier to an unauthorized use is raised further.
[0287]In the device of the 8th inventionbetween different semiconductor substratessince numerals are exchanged in the enciphered formnumerals cannot be read in the exterior. For this reasonthe barrier to an unauthorized use is raised further.
[0288]In the device of the 9th inventionsince a key is generated using dispersion in the electrical property of a semiconductor devicethe semiconductor device manufactured at the same process can be used between these devices of a large number mass-produced. For this reasonmanufacture of a device is simplified. Since the electrical property of the semiconductor device which becomes a basis of a key cannot be changed from the outsidethe barrier to an unjust change of a key is expensive.
[0289]Since a semiconductor device has the polycrystalline substance and a key is generated in the device of the 10th invention using dispersion in the crystal structuredispersion in the electrical property between the semiconductor devices manufactured at the same process is large. For this reasonit is easy to keep a key from being mutually in agreement between these devices of a large number mass-produced.
[0290]Since a key generation part memorizes a key to OTPROM in the device of the 11th inventionthe barrier to an unjust change of the key which a key generation part generates is expensive.
[0291]In the device of the 12th inventionsince a switching circuit is equippedthe identification signal outputted from a semiconductor substrate can be made to look like a memory codeand the unauthorized use made by inputting into the same semiconductor substrate as it is can be prevented.
[0292]responding to the result of comparison by making a prescribed circuit into the part of the circuit which realizes the function of an applied machinesince the prescribed circuit which contains the circuit part which is operation or un-operating based on the judgment of a comparison circuit in the device of the 13th invention is equipped -- predetermined operation of an applied machine -- permission -- and

disapproval can be carried out.
[0293]In the device of the 14th inventionsince the prescribed circuit is formed in one of the semiconductor substrates in which the code generating part and the comparison circuit are formedabout the decision signal inputted into a prescribed circuit from a comparison circuit in the same semiconductor substratethis cannot be inputted from the outside. For this reasonthe barrier to an unauthorized use is raised further.
[0294]In the device of the 15th inventiona code generating part is formed in one side of two semiconductor substratesa memory is formed in another sideand it has the simplest composition [say / that the numerals which are in agreement with an identification signal peculiar to one semiconductor substrate are memorized by the semiconductor substrate of another side]. For this reasonmanufacture of a device is easy and it is possible to miniaturize a device.
[0295]In the device of the 16th inventiona code generating part and a memory are formed in all of two semiconductor substratesand the barrier to an unauthorized use can be raised furtherholding down the number of a semiconductor substrate to the minimumsince the numerals whose two semiconductor substrates correspond with the identification signal of the other party mutually are memorized.
[0296]Since data can be exchanged between the exteriors in the enciphered form in the device of the 17th inventionthe barrier to disclosure of the information which data expresses is expensive. And since the key for encryption is generated using dispersion in the electrical property of a semiconductor devicethe semiconductor device manufactured at the same process can be used between these devices of a large number mass-produced. For this reasonmanufacture of a device is simplified. Since the electrical property of the semiconductor device which becomes a basis of a key cannot be changed from the outsidethe barrier to an unjust change of a key is expensive.
[0297]Since the key generation part is included in the auxiliary section which can be freely detached and attached to a body part in the device of the 18th inventionit is possible to use the same key to two or more body parts.
[0298]Since the key generation part is included in the IC card in the device of the 19th inventionit is convenient to carry.
[0299]Since a semiconductor device has the polycrystalline substance and a key is generated in the device of the 20th invention using dispersion in the crystal structuredispersion in the electrical property between the semiconductor devices manufactured at the same process is large. For this reasonit is easy to keep a key from being mutually in agreement between these devices of a large number mass-produced.
[0300]Since the communication circuit which stops either [at least] transmission or reception is equipped in the device of the 21st invention when the judgment of a comparison circuit shows disagreementIt is automatically stopped by work of the

terminal unit itselfwithout the malfeasance of exchanging a semiconductor substrate and using it for communication waiting for processing by communication enterprise equipment etc.

[0301]In the device of the 22nd inventionsince each decision signal is transmittedwhen communication enterprise equipment etc. perform authenticating processing based on a decision signalthe malfeasance of exchanging a semiconductor substrate and using it for communication can be prevented.

[0302]In the device of the 23rd inventionsince each identification signal and each memory code are transmittedcommunication enterprise equipment etc. compare these numerals and the malfeasance of exchanging a semiconductor substrate and using it for communication can be prevented by performing authenticating processing based on the result.

[0303]In the device of the 24th inventionsince the memory is included in the auxiliary section which can be freely detached and attached to a body partcommunication enterprise equipment etc. can perform attestation with a different level between two kinds when [at which the body part and the auxiliary section joined together] not having joined together at the time. By for exampleattestation of a high level when a body part and an auxiliary section combine communication enterprise equipment. Telex rate gold to communication before it can be recorded as what was able to be supportedand it becomes possible to prevent the illegal act which escapes the obligation to pay a fee [loss of a terminal unit] by that cause.

[0304]Since an identification signal and a memory code are transmitted in the enciphered form in the device of the 25th inventionthe barrier to disclosure of these numerals is expensive.

[0305]In the device of the 26th inventionsince the 1st key generation part and the 1st enciphering circuit are formed in the single semiconductor substrate with the coding circuitan identification signal and the barrier to disclosure of the 1st key are raised further.

[0306]In the device of the 27th inventionsince the 2nd key generation part and the 2nd enciphering circuit are formed in the single semiconductor substrate with the memorya memory code and the barrier to disclosure of the 2nd key are raised further.

[0307]In the device of the 28th inventioncombination with a body part and an auxiliary section is performed periodicallywithout requiring time and effort special to a usersince the auxiliary section is a battery charger which charges the cell of a body part.

[0308]It is that which has an auxiliary section by an IC card in the device of the 29th inventionand is convenient to carry. Since numerals are exchanged on radio between a body part and an auxiliary sectionboth combination is realized only by carrying an IC card with a body part.

[0309]In the device of the 30th inventionsince the communication circuit is formed in one of the semiconductor substrates in which the code generating part is

formedabout the decision signal or numerals inputted into a communication circuit in the same semiconductor substratethis cannot be inputted from the outside. For this reasonthe barrier to an unauthorized use is raised further.

[0310]In the space through which the crowd who carries this device gathers thru/or passes in the device of the 31st inventionA wireless communication network can be formed between these devices which two or more [in a crowd / at least some] carryand even if the field which cannot perform radio which carried communication enterprise equipment by that causefor examplean underground center etc.is in the above-mentioned spacecommunication in the above-mentioned space is attained.

[0311]In the device of the 32nd inventionsince a switching circuit is equippedcommunication of the others which lead a wireless communication network can not only be relayedbut the user of this device itself can perform communication by a wireless communication network.

[0312]Since signal transmission is exchanged in the form which the common key was set up and enciphered in the device of the 33rd invention based on the common key concerned by exchanging a communications partner and numeralsthe barrier to disclosure of a communication content with arbitrary communications partners is expensive.

[0313]In the device of the 34th inventionsince the numerals which become a basis of a common key are generated using dispersion in the electrical property of a semiconductor devicethe semiconductor device manufactured at the same process can be used between these devices of a large number mass-produced. For this reasonmanufacture of a device is simplified. Since the electrical property of the semiconductor device which becomes a basis of numerals cannot be changed from the outsidethe barrier to an unjust change of numerals is expensive.

[0314]Since a semiconductor device has the polycrystalline substance and numerals are generated in the device of the 35th invention using dispersion in the crystal structuredispersion in the electrical property between the semiconductor devices manufactured at the same process is large. For this reasonit is easy to keep numerals from being mutually in agreement between these devices of a large number mass-produced.

[0315]Since a code generating part memorizes numerals to OTPROM in the device of the 36th inventionthe barrier to an unjust change of the numerals which a code generating part generates is expensive.

[0316]In the device of the 37th inventionsince it becomes irregular after getting overand the signal which the wireless communication network circuit received is told to a communication circuitthe utilization ratio of the frequency band of a communication circuit is raised.

[0317]In the method of the 38th inventionsince each decision signal which a terminal unit transmits is used for attestationthe malfeasance of exchanging a semiconductor substrate and using it for communication can be prevented.

[0318]In the method of the 39th inventionsince each identification signal and each memory code which a terminal unit transmits are used for attestationthe malfeasance of exchanging a semiconductor substrate and using it for communication can be prevented.
[0319]In the method of the 40th inventionsince each identification signal and each memory code which were received are recordedthe effect which deters the crime by unauthorized use a priori is acquired. When there is an unauthorized useit becomes possible to use each numerals currently recorded for an unauthorized use person's specification.
[0320]In the method of the 41st inventionsince each identification signal and each memory code which were received are recorded when not attesting at an attestation process (i.e.when a user may be an unauthorized use person)each recorded numerals can be used for an unauthorized use person's specification.
[0321]In the method of the 42nd inventionattestation with a different level between two kinds when [at which the body part and the auxiliary section joined together] not having joined together at the time is performed. the high-ranking attestation made when a body part and an auxiliary section join together -- both an identification signal and a memory code -- although -- since it is made only within the case of being in agreement with the registered numeralsit proves that the accuracy for which the terminal unit is used justly is higher. Thereforecommunication enterprise equipment becomes possible [using the attestation according to the importance of procedure properly].
[0322]Since the memory code which should be registered by communicating where a body part is equipped with an auxiliary section is sent to communication enterprise equipmentin frontthe method of the 43rd invention is sufficientif only an identification signal is registeredrather than a terminal unit includes a user's hand.
[0323]In the method of the 44th inventionsince it is possible to change the 2nd registration codethe user can exchange auxiliary sections if neededafter a terminal unit's coming to hand.
[0324]In the method of the 45th inventionattestation with a different level between two kinds when [at which the body part and the auxiliary section joined together] not having joined together at the time is performed. the high-ranking attestation made when a body part and an auxiliary section join together -- both an identification signal and a memory code -- although -- since it is made only within the case of being in agreement with the registered numeralsit proves that the accuracy for which the terminal unit is used justly is higher. Thereforecommunication enterprise equipment becomes possible [using the attestation according to the importance of procedure properly]. And since an identification signal and a memory code are transmitted in the enciphered formthe barrier to disclosure of these numerals is expensive.
[0325]Since the memory code which should be registered by communicating where a body part is equipped with an auxiliary section is sent to communication enterprise

equipmentin frontthe method of the 46th invention is sufficientif only an identification signal is registeredrather than a terminal unit includes a user's hand.
[0326]In the method of the 47th inventionsince it is possible to change the 2nd registration codethe user can exchange auxiliary sections if neededafter a terminal unit's coming to hand.
[0327]In the method of the 48th inventionsince each identification signal and each memory code which were received are recorded when not attesting at a high-ranking attestation process (i.e.when a possibility that a user is an unauthorized use person is high)each recorded numerals can be used for an unauthorized use person's specification.
[0328]In the method of the 49th inventionin a high rank attestation processwhen performing high-ranking attestation (i.e.when a possibility that a user is a just user is high)Since telex rate gold to communication before it is recorded as what was able to be supportedit is possible to prevent the illegal act which escapes the obligation to pay a fee [loss of a terminal unit].
[0329]In the method of the 50th inventionsince the decision result made at the past high-ranking attestation process is reflected in the usual attestation made in the state where a body part is not equipped with an auxiliary sectionimportant proceduresuch as a commercial transactioncan be performed under the usual attestation.
[0330]In the method of the 51st inventionin a high rank attestation processsince enactment or failure of the commercial transaction performed by communication before it is recorded according to whether high-ranking attestation is performedthe damage caused by the unjust commercial transaction based on the unauthorized use of a terminal unit can be canceled thru/or reduced.
[0331]In the method of the 52nd inventionin an attestation processsince it responds to whether it attests or not and communication is continued or stoppedthe communication based on the unauthorized use of a terminal unit can be prevented.
[0332]In the space through which the crowd who carries the terminal unit which has a predetermined function in the method of the 53rd invention gathers thru/or passesA wireless communication network is formed between the above-mentioned terminal units which two or more [in a crowd / at least some] carryand even if the field which cannot perform radio which carried communication enterprise equipment by that causefor examplean underground center etc.is in the above-mentioned spacecommunication in the above-mentioned space is realized.
[0333]By performing radio in which some of two or more terminal units which form a wireless communication network carried communication enterprise equipment in the method of the 54th inventionSince it is possible to perform communication in which some of two or more of other above-mentioned terminal units carried a wireless communication network and communication enterprise equipmentit becomes possible to perform radio which carried communication enterprise equipment from the field

which cannot perform radio which carried communication enterprise equipmentfor examplean underground center etc.

[0334]Since signal transmission is exchanged in the form which the common key was set up and enciphered in the method of the 55th invention based on the common key concerned by exchanging a communications partner and numeralsthe barrier to disclosure of a communication content with arbitrary communications partners is expensive.

[0335]Since communication which carried the wireless communication network is enabled only within urgent emergency trafficsuch as a request etc. of the rescue accompanying generating of the state of emergency which threatens a life and propertyfor examplethe method of the 56th invention does not take proceduressuch as encryption for preventing disclosure of a communication content.

[0336]Since the terminal unit which can form a wireless communication network is installed in the method of the 57th invention in the field which cannot perform radio which carried communication enterprise equipmentfor examplean underground center etc.In a described areaeven when the density of the crowd who carries the terminal unit which has a predetermined function is lowthe communication which carried the wireless communication network is attained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a block diagram of the semiconductor device of Embodiment 1.

[Drawing 2]It is a block diagram of the code generating part of drawing 1.

[Drawing 3]It is a top view of the semiconductor device of drawing 2.

[Drawing 4]It is the sectional view which met the A–A cutout line of the semiconductor device of drawing 3.

[Drawing 5]It is a top view of the semiconductor device of drawing 2.

[Drawing 6]It is a graph showing the characteristic of the semiconductor device of drawing 2.

[Drawing 7]It is a block diagram of another example of the code generating part of drawing 1.

[Drawing 8]It is a block diagram of the memory of drawing 1.

[Drawing 9]It is a block diagram of the terminal unit of Embodiment 1.

[Drawing 10]It is a block diagram of the communication circuit of drawing 9.

[Drawing 11]It is a flow chart of a procedure until it results in use of the terminal unit of drawing 9.

[Drawing 12]It is a block diagram of the communications system of Embodiment 1.

[Drawing 13]It is a block diagram of the semiconductor device of Embodiment 2.

[Drawing 14]It is a block diagram of the terminal unit of Embodiment 2.

[Drawing 15]It is a flow chart of a procedure until it results in use of the terminal unit of drawing 13.
[Drawing 16]It is a block diagram of the terminal unit of Embodiment 3.
[Drawing 17]It is a flow chart of a correspondence procedure using the terminal unit of drawing 16.
[Drawing 18]It is a block diagram of another example of the terminal unit of Embodiment 3.
[Drawing 19]It is a flow chart of a correspondence procedure using the terminal unit of drawing 18.
[Drawing 20]It is a block diagram of the terminal unit of Embodiment 4.
[Drawing 21]It is a flow chart of a correspondence procedure using the terminal unit of drawing 20.
[Drawing 22]It is a block diagram of another example of the terminal unit of Embodiment 4.
[Drawing 23]It is a flow chart of a correspondence procedure using the terminal unit of drawing 22.
[Drawing 24]It is a block diagram of the semiconductor device of Embodiment 5.
[Drawing 25]It is a block diagram of the key generation part of drawing 24.
[Drawing 26]It is a block diagram of another example of the key generation part of drawing 24.
[Drawing 27]It is a flow chart of a procedure until it results in use of the terminal unit incorporating the semiconductor device of drawing 24.
[Drawing 28]It is a block diagram of another example of the semiconductor device of Embodiment 5.
[Drawing 29]It is a flow chart of a procedure until it results in use of the terminal unit incorporating the semiconductor device of drawing 28.
[Drawing 30]It is a block diagram of the semiconductor device of Embodiment 6.
[Drawing 31]It is a block diagram of the terminal unit of Embodiment 7.
[Drawing 32]It is a block diagram of another example of the terminal unit of Embodiment 7.
[Drawing 33]It is a block diagram of the terminal unit of Embodiment 8.
[Drawing 34]It is a flow chart of a procedure until it results in use of the terminal unit of drawing 33.
[Drawing 35]It is a flow chart of Step S509 of drawing 34.
[Drawing 36]It is a flow chart of Step S509 of drawing 34.
[Drawing 37]It is a block diagram of the terminal unit of Embodiment 9.
[Drawing 38]It is a flow chart of a procedure until it results in use of the terminal unit of drawing 37.
[Drawing 39]It is a flow chart of Step S709 of drawing 38.
[Drawing 40]It is a flow chart of Step S709 of drawing 38.
[Drawing 41]It is a flow chart of another example of Step S709 of drawing 38.

[Drawing 42]It is a flow chart of Step S742 of drawing 41.
[Drawing 43]It is a flow chart of Step S742 of drawing 41.
[Drawing 44]It is a flow chart of another example of Step S709 of drawing 38.
[Drawing 45]It is a flow chart of another example of Step S709 of drawing 38.
[Drawing 46]It is a block diagram of another example of the terminal unit of Embodiment 9.
[Drawing 47]It is an explanatory view of the correspondence procedure of Embodiment 10.
[Drawing 48]It is a block diagram of the terminal unit of Embodiment 10.
[Drawing 49]It is a block diagram of another example of the terminal unit of Embodiment 10.
[Drawing 50]It is a block diagram of the key generation part of drawing 49.
[Drawing 51]It is a flow chart of the key generation by the terminal unit of drawing 49.
[Drawing 52]It is a block diagram of another example of the terminal unit of Embodiment 10.
[Drawing 53]It is an explanatory view of the terminal unit of drawing 52 of operation.
[Drawing 54]It is an explanatory view showing the operation contrasted with drawing 53.
[Drawing 55]It is an explanatory view of another example of the correspondence procedure of Embodiment 10.
[Drawing 56]It is an explanatory view of the correspondence procedure of Embodiment 11.
[Drawing 57]It is a block diagram of the semiconductor device of Embodiment 12.
[Drawing 58]It is an explanatory view of the semiconductor device of drawing 57 of operation.
[Drawing 59]It is a block diagram of the semiconductor device of Embodiment 12.
[Drawing 60]They are some block diagrams of the coding circuit of drawing 59.
[Drawing 61]It is a block diagram of another example of the semiconductor device of Embodiment 12.
[Drawing 62]It is a block diagram of another example of the semiconductor device of Embodiment 12.
[Drawing 63]It is a block diagram of the comparison circuit of the semiconductor device of Embodiment 12.
[Drawing 64]It is a figure explaining processing of the conventional communications system.
[Drawing 65]It is a block diagram of the conventional communication terminal.
[Description of Notations]
400 A code generating part and 401 A semiconductor device and 402 A coding circuit and 403 Comparison circuit405405a A prescribed circuit and 601654 A memory602 OTPROM633676853 A key generation part and 631851 Enciphering circuit632852 A decoding circuit641 switching circuitsand 652672828692 Body part653673693 A

battery charger (auxiliary section) and 655675 Communication enterprise equipment694695 communication interfaces829 IC cards (auxiliary section)841861 A communication circuit846871 wireless LAN circuits (wireless communication network circuit)856870 A switching circuit and 857 Key operation part and 868873 MixerCdCd1and Cd2 An identification signalCoCo1and Co2 Memory codeCH1-CH6CH10-CH13CH20-CH23CH40-CH42CH50-CH52CH70CH71CH90-CH92and CH100-CH104 A semiconductor substrateKK1and K2 Key.